ETSI TS 134 229-1 V10.4.0 (2014-01)

Universal Mobile Telecommunications System (UMTS);
LTE;
Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP);
User Equipment (UE) conformance specification;
Part 1: Protocol conformance specification
(3GPP TS 34.229-1 version 10.4.0 Release 10)

Reference
RTS/TSGR-0534229-1va40

Keywords
LTE,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

The present document is the first part of a multi-part conformance specification valid for 3GPP Release 5 and later releases.

3GPP TS 34.229-1 (the present document): Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); User Equipment (UE) conformance specification; Part 1: Protocol conformance specification- current document.

3GPP TS 34.229-2 [5]: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); User Equipment (UE) conformance specification; Part 2: Implementation Conformance Statement (ICS) proforma specification".

3GPP TS 34.229-3 [6]: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); User Equipment (UE) conformance specification; Part 3: Abstract Test Suites (ATS)".

NOTE 1: The ATS is written in a standard testing language, TTCN-3, as defined in ETSI ES 201 873 Parts 1 to 3 [36] [37] [38].

NOTE 2: For conformance testing of the UTRAN requirements refer to 3GPP TS 34.123 Parts 1 to 3 [2] [3] [4].

NOTE 3: Further information on testing can be found in ETSI ETS 300 406[9] and ISO/IEC 9646-1 [7].

For at least a minimum set of services, the prose descriptions of test cases will have a matching detailed test case implemented in TTCN-3 (and provided in 3GPP TS 34.229-3 [6]).

1 Scope

The present document specifies the protocol conformance testing for the User Equipment (UE) supporting the Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP).

This is the first part of a multi-part test specification. The following information can be found in this part:

- the overall test structure;
- the test configurations;
- the conformance requirement and reference to the core specifications;
- the test purposes; and
- a brief description of the test procedure, the specific test requirements and short message exchange table.

The following information relevant to testing can be found in accompanying specifications:

- the applicability of each test case [5].

A detailed description of the expected sequence of messages can be found in the 3rd part of present test specification [6].

The Implementation Conformance Statement (ICS) pro-forma can be found in the 2nd part of the present test specification [5].

The present document is valid for UE implemented according to 3GPP Releases starting from Release 5 up to the Release indicated on the cover page of the present document.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.
  - For a Release 5 UE, references to 3GPP documents are to version 5.x.y, when available.
  - For a Release 6 UE, references to 3GPP documents are to version 6.x.y, when available.
  - For a Release 7 UE, references to 3GPP documents are to version 7.x.y, when available.
  - For a Release 8 UE, references to 3GPP documents are to version 8.x.y, when available.
  - For a Release 9 UE, references to 3GPP documents are to version 9.x.y, when available.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 34.123-1: "User Equipment (UE) conformance specification; Part 1: Protocol conformance specification".

[3] 3GPP TS 34.123-2: "User Equipment (UE) conformance specification; Part 2: Implementation Conformance Statement (ICS) proforma specification".

[4] 3GPP TS 34.123-3: "User Equipment (UE) conformance specification; Part 3: Abstract Test Suites (ATS)".

[5] 3GPP TS 34.229-2: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); User Equipment (UE) conformance specification; Part 2: Implementation Conformance Statement (ICS) proforma specification".

[6] 3GPP TS 34.229-3: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); User Equipment (UE) conformance specification; Part 3: Abstract Test Suites (ATS)".

[7] ISO/IEC 9646-1: "Information technology - Open systems interconnection - Conformance testing methodology and framework - Part 1: General concepts".

[8] ISO/IEC 9646-7: "Information technology - Open systems interconnection - Conformance testing methodology and framework - Part 7: Implementation Conformance Statements".

[9] ETSI ETS 300 406: "Methods for testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

[10] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[11] 3GPP TS 26.234: " Transparent end-to-end Packet-switched Streaming Service (PSS); Protocols and codecs ".

[12] 3GPP TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols; Stage 3".

[13] 3GPP TS 33.102: "3GPPSecurity; Security architecture".

[14] 3GPP TS 33.203: "Access security for IP based services".

[15] RFC 3261: "SIP: Session Initiation Protocol".

[16] RFC 2617: "HTTP Authentication: Basic and Digest Access Authentication".

[17] RFC 3310: "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

[18] RFC 3455: "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)"

[19] RFC 3608: "Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration".

[20] RFC 3327: "Session Initiation Protocol Extension Header Field for Registering Non-Adjacent Contacts".

[21] RFC 3329: "Security Mechanism Agreement for the Session Initiation Protocol (SIP)".

[22] RFC 3680: "A Session Initiation Protocol (SIP) Event Package for Registrations".

[23] RFC 3315: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[24] RFC 3320: 'Signalling Compression (SigComp)'

[25] RFC 3485: 'The Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Static Dictionary for Signalling Compression (SigComp)'

[26] RFC 3486: 'Compressing the Session Initiation Protocol (SIP)'

[27] RFC 4566: "SDP: Session Description Protocol".

[28] RFC 2403: "The Use of HMAC-MD5-96 within ESP and AH".

[29] RFC 2404: "The Use of HMAC-SHA-1-96 within ESP and AH".

[30] RFC 3264: "An Offer/Answer Model with the Session Description Protocol (SDP)".

[31] RFC 3312: "Integration of Resource Management and Session Initiation Protocol (SIP)".

[32] 3GPP TS 23.003: "Numbering, addressing and identification".

[33] RFC 3262: "Registration of provisional responses in Session Initiation Protocol (SIP)".

[34] RFC 3265: "Session Initiation Protocol (SIP) Specific Event Notification".

[35] 3GPP TR 23.981 'Universal Mobile Telecommunications System (UMTS); Interworking aspects and migration scenarios for IPv4-based IP Multimedia Subsystem (IMS) implementations'.

[36] ETSI ES 201 873-1: "Methods for Testing and Specification (MTS); The Testing and Test Control Notation version 3; Part 1: TTCN-3 Core Language'.

[37] ETSI ES 201 873-2: "Methods for Testing and Specification (MTS); The Testing and Test Control Notation version 3; Part 2: TTCN-3 Tabular Presentation Format (TFT)".

[38] ETSI TR 201 873-3: "Methods for Testing and Specification (MTS); The Testing and Test Control Notation version 3; Part 3: TTCN-3 Graphical Presentation Format (GFT)".

[39] 3GPP TS 22.101: "Service aspects; Service principles".

[40] 3GPP TS 34.108: "Common test environments for User Equipment (UE); Conformance testing".

[41] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[42] 3GPP TS 27.060: "Packet domain; Mobile Station (MS) supporting Packet Switched services".

[43] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[44] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[45] 3GPP TS 29.207: "Policy control over Go interface".

[46] 3GPP TS 29.208: "End-to-end Quality of Service (QoS) signalling flows".

[47] RFC 2373: "IP Version 6 Addressing Architecture".

[48] RFC 3646: "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[49] RFC 2132: "DHCP Options and BOOTP Vendor Extensions "

[50] RFC 3263: "Session Initiation Protocol (SIP): Locating SIP Servers".

[51] RFC 3319: "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers".

[52] RFC 1035: "Domain Names - Implementation And Specification".

[53] RFC 3556: "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth".

[54] RFC 2833: "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".

[55] RFC 2131: "Dynamic Host Configuration Protocol".

[56] RFC 2782: "A DNS RR for specifying the location of services (DNS SRV)".

[57] RFC 3361: "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers".

[58] 3GPP TS 25.331: "Radio Resource Control (RRC) protocol specification".

[59] 3GPP TR 33.978: "Security aspects of early IP Multimedia Subsystem (IMS)".

[60] RFC 3903: " Session Initiation Protocol (SIP) Extension for EventState Publication".

[61] RFC 5627: "Obtaining and Using Globally Routable User Agent (UA) URIs (GRUU) in the Session Initiation Protocol (SIP)".

[62] RFC 5628: "Reg Event Package Extension for GRUUs".

[63] RFC 3840: "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)"

[64] RFC 3841: "Caller Preferences for the Session Initiation Protocol (SIP)".

[65] 3GPP TS 24.173: "IMS Multimedia Telephony Communication Service and supplementary services; stage 3"

[66] 3GPP TS 26.114: "IP Multimedia Subsystem (IMS); Multimedia Telephony; Media handling and interaction".

[67] RFC 4867: "RTP Payload Format and File Storage Format for the Adaptive Multi-Rate (AMR) and Adaptive Multi-Rate Wideband (AMR-WB) Audio Codecs".

[68] IETF RFC 6050: "A Session Initiation Protocol (SIP) Extension for the Identification of Services".

[69] RFC 2616: "Hypertext Transfer Protocol -- HTTP/1.1".

[70] RFC 4825: "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)".

[71] RFC 4745: "Common Policy: A Document Format for Expressing Privacy Preferences".

[72] RFC 3515: "The Session Initiation Protocol (SIP) Refer Method".

[73] RFC 4032: "Update to the Session Initiation Protocol (SIP) Preconditions Framework".

[74] 3GPP TS 24.423: "PSTN/ISDN simulation services; Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating NGN PSTN/ISDN Simulation Services".

[75] 3GPP TS 24.407: "PSTN/ISDN simulation services; Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR); Protocol specification".

[76] 3GPP TS 24.408: "PSTN/ISDN simulation services; Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR); Protocol specification".

[77] 3GPP TS 24.404: "PSTN/ISDN simulation services: Communication Diversion (CDIV); Protocol specification".

[78] 3GPP TS 24.411: "PSTN/ISDN simulation services: Anonymous Communication Rejection (ACR) and Communication Barring (CB); Protocol specification".

[79] 3GPP TS 24.405: "PSTN/ISDN simulation services: Conference (CONF); Protocol specification".

[80] 3GPP TS 24.406: "PSTN/ISDN simulation services: Message Waiting Indication (MWI): Protocol specification".

[81] 3GPP TS 24.410: "PSTN/ISDN simulation services: Communication HOLD (HOLD); PSTN/ISDN simulation services".

[82] 3GPP TS 24.429: "PSTN/ISDN simulation services: Explicit Communication Transfer (ECT); Protocol specification".

[83] RFC 4244: "An Extension to the Session Initiation Protocol (SIP) for Request History Information".

[84] 3GPP TS 24.147: "Conferencing using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[85] IETF RFC 4353: "A Framework for Conferencing with the Session Initiation Protocol (SIP)".

[86] IETF RFC 4575: "A Session Initiation Protocol (SIP) Event Package for Conference State".

[87] 3GPP TS 24.247: "Messaging service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3".

[88] IETF RFC 3842: "A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)".

[89] IETF RFC 3325: "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks".

[90] 3GPP TS 24.341: "Support of SMS over IP networks; Stage 3".

[91] IETF RFC 3428: "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[92] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[93] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[94] 3GPP TS 36.508: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access (E-UTRAN); Common Test Environments for User Equipment (UE) Conformance Testing".

[95] 3GPP TS 24.615: "Communication Waiting (CW) using IP Multimedia (IM) Core Network (CN) subsystem".

[96] IETF RFC 3581: "An Extension to the Session Initiation Protocol (SIP) for Symmetric Response Routing".

[97] IETF RFC 5031: "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services".

[98] RFC 6442 (December 2011): "Location Conveyance for the Session Initiation Protocol".

[99] IETF RFC 4119: "A Presence-based GEOPRIV Location Object Format".

[100] draft-patel-ecrit-sos-parameter-08 (February 2010): "SOS Uniform Resource Identifier (URI) parameter for marking of Session Initiation Protocol (SIP) requests related to emergency services".

[101] 3GPP TS 24.611: "Anonymous Communication Rejection (ACR) and Communication Barring (CB) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[102] 3GPP TS 24.607: "Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[103] 3GPP TS 24.608: "Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[104] 3GPP TS 24.629: "Explicit Communication Transfer (ECT) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[105] 3GPP TS 24.623: "Extensible Markup Language (XML) Configuration Access Protocol (XCAP) over the Ut interface for Manipulating Supplementary Services ".

[106] 3GPP TS 24.604: "Communication Diversion (CDIV) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[107] 3GPP TS 24.606: "Message Waiting Indication (MWI) using IP Multimedia (IM) Core Network (CN) subsystem: Protocol specification".

[108] 3GPP TS 24.610: " Communication HOLD (HOLD) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification".

[109] IETF RFC 5626: "Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)".

[110] 3GPP TS 24.237: 'IP Multimedia (IM) Core Network (CN) subsystem IP Multimedia Subsystem (IMS) Service Continuity'

[111] 3GPP TS 36. 523-1: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Packet Core (EPC); User Equipment (UE) conformance specification; Part 1: Protocol conformance specification".

[112] 3GPP2 C.S0005-E: 'Upper Layer (Layer 3) Signalling Standard for cdma2000 Spread Spectrum Systems'

[113] 3GPP TS 31.121: "UICC-terminal interface; Universal Subscriber Identity Module (USIM) application test specification".

[114] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification".

[115] draft-kaplan-dispatch-session-id-00 (December 2009): "A Session Identifier for the Session Initiation Protocol (SIP)".

[116] Void.

[117] 3GPP TS 34.109: "Terminal logical test interface; Special conformance testing functions".

[118] 3GPP TS 36.509: 'Special conformance testing functions for User Equipment (UE)".

[119] 3GPP TS 24.109: "Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details".

[120] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[121] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[122] draft-montemurro-gsma-imei-urn-19: "A Uniform Resource Name Namespace for the GSM Association (GSMA) and the International Mobile station Equipment Identity (IMEI)"

Editor's note: The above document cannot be formally referenced until it is published as an RFC.

3 Definitions, symbols and abbreviations

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

3.1 Definitions

For the purposes of the present document, the following additional definitions apply:

Example: text used to clarify abstract rules by applying them literally

Floor: Floor(x) is the largest integer smaller than or equal to x.

Ceil: Ceil (x) is the smallest integer larger than or equal to x.

3.2 Symbols

For the purposes of the present document, the following additional symbols apply:

None.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AAAA	Address (IP v6)
AKA	Authentication and Key Agreement
AKAv1-MD5	Authentication and Key Agreement version 1- Message-Digest 5
DUID	DHCP Unique Identifier
EF	Elementary File
FQDN	Fully Qualified Domain Name
HMAC-MD5-96	Hashing for Message Authentication Code - Message-Digest 5 – 96 (bits)
HMAC-SHA-1-96	Hashing for Message Authentication Code - Secure Hash Algorithm 1 - 96 (bits)
ICS	Implementation Conformance Statement
IN	INternet
IPsec	IP Security
IXIT	Implementation eXtra Information for Testing
MIME	Multi purpose Internet Mail Extensions
MF	Master File
NAPTR	Naming Authority Pointer
P-CSCF	Proxy – Call Session Control Function
RTCP	Real Time Transport Control Protocol
SIGComp	SIGnalling Compression
SRV	SeRVice
SS	System Simulator

4 Overview

4.1 Test Methodology

4.1.1 Testing of optional functions and procedures

Any function or procedure which is optional, as indicated in the present document may be subject to a conformance test if it is implemented in the UE.

A declaration by the apparatus supplier (Implementation Conformance Statement (ICS)) is used to determine whether an optional function/procedure has been implemented (see ISO/IEC 9646-7 [8] for general information about ICS).

4.2 Implicit Testing

For some 3GPP signalling and protocol features conformance is not verified explicitly in the present document. This does not imply that correct functioning of these features is not essential, but that these are implicitly tested to a sufficient degree in other tests.

4.3 Conformance Requirements

The Conformance Requirements clauses in the present document are copy/paste from the relevant core specification where skipped text has been replaced with "...". References to clauses in the Conformance Requirements section of the test body refers to clauses in the referred specification, not sections in the present document.

5 Reference Conditions

The test cases are expected to be executed through the 3GPP radio interface. Details of the radio interfaces are outside the scope of this specification. The reference environments used by tests are specified in the test.

5.1 Generic setup procedures

A set of basic generic procedures for PDP Context Activation, P-CSCF Discovery and Registration are described in Annex C. These procedures are used in numerous test cases throughout the present document.

5.2 Transport protocols applied

For simplicity, UDP (*User Datagram Protocol*) is applied to the IMS test as default DL transport protocol.

NOTE: Which UL transport protocol is used in the test is decided by the UE.

6 PDP Context Activation

6.1 General Purpose PDP Context Establishment

Implicitly tested.

NOTE: This is implicitly tested as part of generic procedures.

6.2 General Purpose PDP Context Establishment (UE Requests for a Dedicated PDP Context)

6.2.1 Definition

Test to verify that the UE can establish a "General Purpose PDP context" for SIP signalling. The test case is applicable for GIBA.

6.2.2 Conformance requirement

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure as specified in 3GPP TS 24.008 [8];

b) ensure that a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A] is available. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

NOTE 1: During the PDP context activation procedure, the UE and network negotiate whether the UE or the GPRS IP-CAN is responsible for the resource reservation applicable to all PDP contexts within the activated PDP address/APN pair, as described in 3GPP TS 24.008 [8].

When the bearer establishment is controlled by the UE, the UE shall choose one of the following options when performing establishment of this PDP context:

I. ….

II. A general-purpose PDP context:

The UE may decide to use a general-purpose PDP Context to carry IM CN subsystem-related signalling. The UE shall indicate to the GGSN that this is a general-purpose PDP context by not setting the IM CN Subsystem Signalling Flag. The UE may carry both signalling and media on the general-purpose PDP context. The UE can also set the Signalling Indication attribute within the QoS information element.

NOTE 2: When the bearer establishment is controlled by the GPRS IP-CAN, the GGSN follows the procedures described in 3GPP TS 29.061 [11] in order to establish a dedicated PDP context for SIP signalling.

The UE indicates the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options information element of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message. Upon successful signalling PDP context establishment the UE receives an indication from GGSN in the form of IM CN Subsystem Signalling Flag within the Protocol Configuration Options information element. If the flag is not received, the UE shall consider the PDP context as a general-purpose PDP context.

The encoding of the IM CN Subsystem Signalling Flag within the Protocol Configuration Options information element is described in 3GPP TS 24.008 [8].

Reference(s)

3GPP TS 24.229[10], clause B.2.2.1.

6.2.3 Test purpose

To verify that the UE sends a correctly composed Activate PDP context request by setting the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE.

On receiving Activate PDP Context accept with IM CN Subsystem Signalling Flag not set within the Protocol Configuration Options IE, UE shall consider the PDP context as a General Purpose PDP context for SIP signalling.

6.2.4 Method of test

Initial conditions

The UE is in GMM-state "GMM-REGISTERED, normal service" with valid P-TMSI and CKSN. UE is not registered to IMS services, has not established PDP context for IMS

Related ICS/IXIT Statement(s)

UE capable of being configured to initiate Dedicated PDP Context (Yes/No)

UE Supports IPv4 (Yes/No)

UE Supports IPv6 (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Test procedure

1) UE is configured for setting the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE in Activate PDP Context Request message. UE initiates an Activate PDP Context procedure.

2) SS Responds with an Activate PDP Context Accept message by not setting IM CN Subsystem Signalling Flag within the Protocol Configuration Options IE

3) P-CSCF address discovery using the DHCP procedure according to Annex C.3 for IPv6 or Annex C.4 for IPv4.

4) UE sends an initial REGISTER request.

5) Continue test execution with the Generic test procedure, Annex C.2 or C.2a (GIBA only), step 5.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		Activate PDP Context Request	UE sends this PDU by setting the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE
2	←		Activate PDP Context Accept	SS Sends this response by not setting IM CN Subsystem Signalling Flag within the Protocol Configuration Options IE
3				P-CSCF address discovery using the DHCP procedure according to Annex C.3 for IPv6 or Annex C.4 for IPv4.
4	→		REGISTER	UE sends initial registration for IMS services
5	←→		Continue with Annex C.2 or C.2a step 5	Execute the Generic test procedure Annex C.2 step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state

NOTE: The default messages contents in annex A are used with condition "IMS security" or "GIBA" when applicable

Specific Message Contents:

Activate PDP Context Request (step 1)

IE	Value/Remarks
Protocol Configuration options - Additional Parameters -- container 1 Identifier -- Container 1 Length	 * 0002H (IM CN Subsystem Signalling Flag) 0 bytes

*NOTE: UE may include additional containers also. If multiple containers are present they can be in any order.

Activate PDP Context Accept (step 2)

Case 1: UE supports IPv6 / IPv6 and IPv4

IE	Value/Remarks
Protocol Configuration options - Additional Parameters -- container 1 Identifier -- Container 1 Length -- Container 1 contents -- container 2 Identifier -- Container 2 Length -- Container 2 contents	 0001H (P-CSCF Address) (Included if "P-CSCF Server Address Request" is received) 16 bytes IPV6 address of SS P-CSCF Server 0003H (DNS Address) (Included if "DNS Server Address Request" is received) 16 bytes IPV6 address of SS DNS Server

Case 2: UE supports only IPv4

IE	Value/Remarks
Protocol Configuration options - Additional Parameters -- container 1 Identifier -- Container 1 Length -- Container 1 contents -- container 2 Identifier -- Container 2 Length -- Container 2 contents	 0001H (P-CSCF Address) 16 bytes IPV4 address of SS P-CSCF encoded as per 3GPP TR 23.981[35] 0003H (DNS Address) (Included if "DNS Server Address Request" is received) 16 bytes IPV4 address of SS DNS server encoded as per 3GPP TR23.981[35]

REGISTER (Step 4)

Use the default message 'REGISTER' in annex A.1.1 with condition A1 "Initial unprotected REGISTER"

6.2.5 Test requirements

1) In step 1, the UE shall set the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE.

2) In step 4, the UE shall send an initial REGISTER message using the established PDP context.

6.3 Dedicated PDP Context Establishment

6.3.1 Definition

Test to verify that the UE can establish a "Dedicated PDP context" for SIP signalling. The test case is applicable for IMS security or GIBA.

6.3.2 Conformance requirement

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure as specified in 3GPP TS 24.008 [8];

b) ensure that a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A] is available. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

NOTE 1: During the PDP context activation procedure, the UE and network negotiate whether the UE or the GPRS IP-CAN is responsible for the resource reservation applicable to all PDP contexts within the activated PDP address/APN pair, as described in 3GPP TS 24.008 [8].

When the bearer establishment is controlled by the UE, the UE shall choose one of the following options when performing establishment of this PDP context:

I. A dedicated PDP context for SIP signalling:

The UE shall indicate to the GGSN that this is a PDP context intended to carry IM CN subsystem-related signalling only by setting the IM CN Subsystem Signalling Flag. The UE may also use this PDP context for DNS and DHCP signalling according to the static packet filters as described in 3GPP TS 29.061 [11]. The UE can also set the Signalling Indication attribute within the QoS information element;

II. A general-purpose PDP context:

The UE may decide to use a general-purpose PDP Context to carry IM CN subsystem-related signalling. The UE shall indicate to the GGSN that this is a general-purpose PDP context by not setting the IM CN Subsystem Signalling Flag. The UE may carry both signalling and media on the general-purpose PDP context. The UE can also set the Signalling Indication attribute within the QoS information element.

NOTE 2: When the bearer establishment is controlled by the GPRS IP-CAN, the GGSN follows the procedures described in 3GPP TS 29.061 [11] in order to establish a dedicated PDP context for SIP signalling.

The UE indicates the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options information element of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message. Upon successful signalling PDP context establishment the UE receives an indication from GGSN in the form of IM CN Subsystem Signalling Flag within the Protocol Configuration Options information element. If the flag is not received, the UE shall consider the PDP context as a general-purpose PDP context.

The encoding of the IM CN Subsystem Signalling Flag within the Protocol Configuration Options information element is described in 3GPP TS 24.008 [8].

Reference(s)

3GPP TS 24.229[10], clause B.2.2.1.

6.3.3 Test purpose

To verify that on receiving Activate PDP Context accept with IM CN Subsystem Signalling Flag included within the Protocol Configuration Options IE, UE shall consider the PDP context as a Dedicated PDP context for SIP signalling.

6.3.4 Method of test

Initial conditions

The UE is in GMM-state "GMM-REGISTERED, normal service" with valid P-TMSI and CKSN. UE is not registered to IMS services, has not established PDP context.

Related ICS/IXIT Statement(s)

UE capable of being configured to initiate Dedicated PDP Context (Yes/No)

UE Supports IPv4 (Yes/No)

UE Supports IPv6 (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Test procedure

1) UE is configured for setting the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE in Activate PDP Context Request message. UE initiates an Activate PDP Context procedure.

2) SS Responds with an Activate PDP Context Accept message by including IM CN Subsystem Signalling Flag within the Protocol Configuration Options IE.

3) P-CSCF address discovery using the DHCP procedure according to Annex C.3 for IPv6 or Annex C.4 for IPv4.

4) UE sends an initial REGISTER request.

5) Continue test execution with the Generic test procedure, Annex C.2 or C.2a (GIBA only), step 5.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		Activate PDP Context Request	UE sends this PDU by setting the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE
2	←		Activate PDP Context Accept	SS Sends this response by including IM CN Subsystem Signalling Flag within the Protocol Configuration Options IE
3				P-CSCF address discovery using the DHCP procedure according to Annex C.3 for IPv6 or Annex C.4 for IPv4.
4	→		REGISTER	UE sends initial registration for IMS services
5	←→		Continue with Annex C.2 or C.2a step 5	Execute the Generic test procedure Annex C.2 step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state

NOTE: The default messages contents in annex A are used with condition 'IMS security'or 'GIBA' when applicable

Specific Message Contents:

Activate PDP Context Request (step 1)

IE	Value/Remarks
Protocol Configuration options - Additional Parameters -- container 1 Identifier -- Container 1 Length	 * 0002H (IM CN Subsystem Signalling Flag) 0 bytes

* NOTE: UE may include additional containers also. If multiple containers are present they can be in any order.

Activate PDP Context Accept (step 2)

Case 1: UE supports IPv6 / IPv6 and IPv4

IE	Value/Remarks
Protocol Configuration options - Additional Parameters -- container 1 Identifier -- Container 1 Length -- container 2 Identifier -- Container 2 Length -- Container 2 contents -- container 3 Identifier -- Container 3 Length -- Container 3 contents	 0002H (IM CN Subsystem Signalling Flag) 0 bytes 0001H (P-CSCF Address) (Included if "P-CSCF Server Address Request" is received) 16 bytes IPV6 address of SS P-CSCF Server 0003H (DNS Address) (Included if "DNS Server Address Request" is received) 16 bytes IPV6 address of SS DNS Server

Case 2: UE supports only IPv4

IE	Value/Remarks
Protocol Configuration options	
- Additional Parameters	
-- container 1 Identifier	0002H (IM CN Subsystem Signalling Flag)
-- Container 1 Length	0 bytes
-- container 2 Identifier	0001H (P-CSCF Address)
-- Container 2 Length	16 bytes
-- Container 2 contents	IPV4 address of SS P-CSCF encoded as per 3GPP TR 23.981
-- container 3 Identifier	0003H (DNS Address) (Included if "DNS Server Address Request" is received)
-- Container 3 Length	16 bytes
-- Container 3 contents	IPV4 address of SS DNS server encoded as per 3GPP TR 23.981[35]

REGISTER (Step 4)

Use the default message 'REGISTER' in annex A.1.1 with condition A1 "Initial unprotected REGISTER"

6.3.5 Test requirements

1) In step 1, the UE shall set the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE.

2) In step 4, the UE shall send an initial REGISTER message using the established PDP context.

7 P-CSCF Discovery

7.1 P-CSCF Discovery via PDP Context

7.1.1 Definition

Test to verify that the UE can establish a PDP context for SIP signalling and acquire P-CSCF address(es) during PDP Context Activation procedure. The test case is applicable for IMS security or GIBA.

7.1.2 Conformance requirement

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure as specified in 3GPP TS 24.008 [8];

b) ensure that a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A] is available. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

NOTE 1: During the PDP context activation procedure, the UE and network negotiate whether the UE or the GPRS IP-CAN is responsible for the resource reservation applicable to all PDP contexts within the activated PDP address/APN pair, as described in 3GPP TS 24.008 [8].

When the bearer establishment is controlled by the UE, the UE shall choose one of the following options when performing establishment of this PDP context:

I. …

II. A general-purpose PDP context:

The UE may decide to use a general-purpose PDP Context to carry IM CN subsystem-related signalling. The UE shall indicate to the GGSN that this is a general-purpose PDP context by not setting the IM CN Subsystem Signalling Flag. The UE may carry both signalling and media on the general-purpose PDP context. The UE can also set the Signalling Indication attribute within the QoS information element.

NOTE 2: When the bearer establishment is controlled by the GPRS IP-CAN, the GGSN follows the procedures described in 3GPP TS 29.061 [11] in order to establish a dedicated PDP context for SIP signalling.

The UE indicates the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options information element of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message. Upon successful signalling PDP context establishment the UE receives an indication from GGSN in the form of IM CN Subsystem Signalling Flag within the Protocol Configuration Options information element. If the flag is not received, the UE shall consider the PDP context as a general-purpose PDP context.

The encoding of the IM CN Subsystem Signalling Flag within the Protocol Configuration Options information element is described in 3GPP TS 24.008 [8].

The UE can indicate a request for prioritised handling over the radio interface by setting the Signalling Indication attribute (see 3GPP TS 23.107 [4A]). The general QoS negotiation mechanism and the encoding of the Signalling Indication attribute within the QoS information element are described in 3GPP TS 24.008 [8].

NOTE 3: A general-purpose PDP Context can carry both IM CN subsystem signalling and media, in case the media does not need to be authorized by Policy and Charging control mechanisms as defined in 3GPP TS 29.212 [13C] and Service Based Local Policy mechanisms defined in 3GPP TS 29.207 [12] and the media stream is not mandated by the P-CSCF to be carried in a separate PDP Context.

c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

I. …

II. Transfer P-CSCF address(es) within the PDP context activation procedure.

The UE shall indicate the request for a P-CSCF address to the GGSN within the Protocol Configuration Options information element of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message.

If the GGSN provides the UE with a list of P-CSCF IPv4 or IPv6 addresses in the ACTIVATE PDP CONTEXT ACCEPT message or ACTIVATE SECONDARY PDP CONTEXT ACCEPT message, the UE shall assume that the list is prioritised with the first address within the Protocol Configuration Options information element as the P-CSCF address with the highest priority.

From 3GPP TR 23.981 [35]:

The existing P-CSCF discovery mechanism are either IPv6 specific or use Release 5 or later GPRS. For an IPv4 based IMS implementation, operators may need other mechanisms not currently defined as possible options in 3GPP IMS.

The following mechanisms need to be evaluated for P-CSCF discovery in IPv4:

a) the address of the P-CSCF can be requested by the UE and returned by the GGSN at PDP context establishment time. An IPv4 UE would need to obtain an IPv4 address as part of this exchange.

If the PDP context established is of PDP type IPv4, then the GGSN may provide an IPv4 P-CSCF address. This does not preclude scenarios, where the GGSN returns an IPv6 P-CSCF address at IPv4 PDP context establishment, e.g. for the support of tunnelling (see clause 5.3.4.3), or both IPv4 and IPv6 P-CSCF addresses. If the PDP type is IPv4 then it is recommended that the GGSN always return both IP versions, if it is capable, using the existing capabilities to send multiple P-CSCF addresses within the PCO IE.

According to TS 24.008 [9], the P-CSCF address in the PCO field is an IPv6 address. Thus there are at least two possible approaches: The first approach would be to avoid any changes to or deviations from TS 24.008 [9] and use the existing methods to transfer an IPv4 address as an IPv6 address ("IPv6 address with embedded IPv4 address", as defined in RFC 2373 [10]). In such a case, the use of 'IPv4 mapped addresses' as defined in RFC 2373 [10] is recommended.

The second approach would set the PCO field length to 4 and put the IP address in the content field. This would be a straightforward generalization of the specified method.

Reference(s)

3GPP TS 24.229[10], clause B.2.2.1.

3GPP TR 23.981[35], clause 5.2.1.

7.1.3 Test purpose

To verify that the UE sends a correctly composed Activate PDP context request message requesting for P-CSCF address(es) to the GGSN within the Protocol Configuration Options IE.

On receiving Activate PDP Context accept with IM CN Subsystem Signalling Flag not included within the Protocol Configuration Options IE and list of P-CSCF IPv6/IPv4 addresses included, UE shall consider the PDP context as a general purpose PDP context for SIP signalling and P-CSCF discovery procedure to be successful.

7.1.4 Method of test

Initial conditions

The UE is in GMM-state "GMM-REGISTERED, normal service" with valid P-TMSI and CKSN. UE is not registered to IMS services, has not established PDP context for IMS.

Related ICS/IXIT Statement(s)

UE Supports IPv4 (Yes/No)

UE Supports "IPv6 address with embedded IPv4 address" in PCO IE (Yes/No)

UE Supports IPv4 address in PCO IE (Yes/No)

UE Supports IPv6 (Yes/No)

UE capable of being configured to initiate P-CSCF Discovery via PCO (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Test procedure

1) UE is configured for setting request for a P-CSCF address to the GGSN within the Protocol Configuration Options IE in Activate PDP Context Request message. UE initiates an Activate PDP Context procedure.

2) SS responds with an Activate PDP Context Accept including list of P-CSCF IPv6 and IPv4 addresses. IPv4 addresses are encoded as per 3GPP TR 23.981[35] clause 5.2.1.

3) UE sends an initial REGISTER request.

4) Continue test execution with the Generic test procedure, Annex C.2 or C.2a (GIBA only), step 5.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		Activate PDP Context Request	UE sends this PDU by setting request for P-CSCF address(es) to the GGSN within the Protocol Configuration Options IE
2	←		Activate PDP Context Accept	SS Sends this response by including list of P-CSCF addresses
3	→		REGISTER	UE sends initial registration for IMS services
4	←→		Continue with Annex C.2 or C.2a step 5	Execute the Generic test procedure Annex C.2 or step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state

NOTE: The test sequence is identical for IPv4 and IPv6 except the message contents of Activate PDP Context Accept message. For a UE supporting both IPv4 and IPv6, only IPv6 option need to be executed.

NOTE: The default messages contents in annex A are used with condition 'IMS security ' or 'GIBA' when applicable

Specific Message Contents:

Activate PDP Context Request (step 1)

NOTE: Containers can be in any order.

IE	Value/Remarks
Protocol Configuration options	
- Additional Parameters	
-- container 1 Identifier	0001H (P-CSCF Address Request);
-- Container 1 Length	0 bytes
-- container 2 Identifier	0003H (DNS Server Address Request) (Optional)
-- Container 2 Length	0 bytes

Activate PDP Context Accept (step 2)

Case 1: UE supports IPv6 / IPv6 and IPv4

IE	Value/Remarks
Protocol Configuration options	
- Additional Parameters	
-- container 1 Identifier	0001H (P-CSCF Address)
-- Container 1 Length	16 bytes
-- Container 1 contents	IPV6 address of SS P-CSCF Server
-- container 2 Identifier	0003H (DNS Address) (Included if "DNS Server Address Request" is received)
-- Container 2 Length	16 bytes
-- Container 2 contents	IPV6 address of SS DNS Server

Case 2: UE supports "IPv6 address with embedded IPv4 address" in PCO IE

IE	Value/Remarks
- Additional Parameters	
Protocol Configuration options - Additional Parameters -- container 2 Identifier -- Container 2 Length -- Container 2 contents -- container 3 Identifier -- Container 3 Length -- Container 3 contents	 0001H (P-CSCF Address) 16 bytes IPV4 address of SS encoded as per 3GPP TR 23.981[35] option 1 0003H (DNS Address) (Included if "DNS Server Address Request" is received) 16 bytes IPV4 address of SS DNS server encoded as per 3GPP TR 23.981[35] option 1

Case 3: UE supports IPv4 address in PCO IE

IE	Value/Remarks
- Additional Parameters	
Protocol Configuration options - Additional Parameters -- container 2 Identifier -- Container 2 Length -- Container 2 contents -- container 3 Identifier -- Container 3 Length -- Container 3 contents	 0001H (P-CSCF Address) 4 bytes IPV4 address of SS encoded as per 3GPP TR 23.981[35] option 2 0003H (DNS Address) (Included if "DNS Server Address Request" is received) 4 bytes IPV4 address of SS DNS server encoded as per 3GPP TR 23.981[35] option 2

7.1.5 Test requirements

1) In step 1, the UE shall request for P-CSCF address to the GGSN within the Protocol Configuration Options IE.

2) In step 3, the UE shall send an initial REGISTER message using the discovered P-CSCF address.

7.2 P-CSCF Discovery via DHCP – IPv4

7.2.1 Definition

Test to verify that UE will perform P-CSCF discovery procedure via DHCP. The test case is applicable for IMS security or GIBA.

7.2.2 Conformance requirement

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure as specified in 3GPP TS 24.008 [8];

b) ensure that a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A] is available. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

…

c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

I. When using IPv4, employ the Dynamic Host Configuration Protocol (DHCP) RFC 2132 [20F], the DHCPv4 options for SIP servers RFC 3361 [35A], and RFC 3263 [27A] as described in subclause 9.2.1. When using IPv6, employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 [56C] as described in subclause 9.2.1.

II. …

The UE can freely select method I or II for P-CSCF discovery, if:

- the UE is in the home network; or

- the UE is roaming and the P-CSCF is to be discovered in the visited network .

In case method I is selected and several P-CSCF addresses or FQDNs are provided to the UE, the selection of P-CSCF address or FQDN shall be performed as indicated in RFC 3361 [35A] when using IPv4 or RFC 3319 [41] when using IPv6. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

NOTE 4: The UE decides whether the P-CSCF is to be discovered in the serving network or in the home network based on local configuration, e.g. whether the application on the UE is permitted to use local breakout.

If the UE is designed to use I above, but receives P-CSCF address(es) according to II, then the UE shall either ignore the received address(es), or use the address(es) in accordance with II, and not proceed with the DHCP request according to I.

When using IPv4, the UE may request a DNS Server IPv4 address(es) via RFC 2132 [20F] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

When using IPv6, the UE may request a DNS Server IPv6 address(es) via RFC 3315 [40] and RFC 3646 [56C] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

From 3GPP TR 23.981[35]:

The following mechanisms need to be evaluated for P-CSCF discovery in IPv4:

...

b) based on DHCP. Currently the specifications limit this to the IPv6 methods for DHCP. In order for this method to be used by an IPv4 UE, it needs to be identified how IPv4 DHCP is used to obtain the P-CSCF address. A solution that provides access independence would be that an IPv4 P-CSCF and IPv4 UE support configuration of the appropriate P-CSCF information via DHCPv4. In this solution, use of DHCP provides the UE with the fully qualified domain name of a P-CSCF and the address of a Domain Name Server (DNS) that is capable of resolving the P-CSCF name. When using DHCP/DNS procedure for P-CSCF discovery with IPv4 GPRS-access, the GGSN acts as DHCP Relay agent relaying DHCP messages between UE and the DHCP server. This is necessary to allow the UE to properly interoperate with the GGSN. This solution however requires that a UE supporting early IPv4 implementations would support DHCPv4.

Reference(s)

3GPP TS 24.229[10], clause B.2.2.1.

3GPP TR 23.981[35], clause 5.2.1.

7.2.3 Test purpose

To verify UE shall initiate and successfully complete a P-CSCF discovery procedure via DHCP when P-CSCF address is not provided as part of PDP Context Activation procedure.

7.2.4 Method of test

Initial conditions

The UE is in GMM-state "GMM-REGISTERED, normal service" with valid P-TMSI and CKSN. UE is not registered to IMS services. UE is not configured for using static P-CSCF address. UE has established a PDP context (No P-CSCF address information provided).). If UE sets flag "DNS Server Address Request" in PCO of PDP Context Request, DNS server address list is provided in PDP Context Accept message.

Related ICS/IXIT Statement(s)

UE Supports IPv4 (Yes/No)

UE capable of being configured to initiate P-CSCF Discovery via DHCPv4 (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Test procedure

1) If UE already knows DHCP server address or is configured to send DHCPINFORM message to the limited (all 1s) broadcast address, it goes to step 3. Otherwise, UE sends DHCPDISCOVER message locating a server.

2) SS responds by DHCPOFFER message.

3) UE sends DHCPINFORM message requesting for P-CSCF address(es) in options field.

4) SS responds by DHCPACK message providing the domain names of P-CSCF address(es) and giving DNS server address.

5) UE initiates a DNS NAPTR query to select the transport protocol. UE"s configured to use specific Transport protocol on default ports, can skip steps 5 to 8 and go directly to step 9.

6) SS responds with NAPTR response.

7) UE initiates a DNS SRV query.

8) SS responds with SRV response.

9) UE initiates a DNS A query

10) SS responds with DNS A response.

11) UE sends an initial REGISTER request.

12) Continue test execution with the Generic test procedure, Annex C.2, step 5.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		DHCPDISCOVER	Optionally sent if UE does not have DHCP server address and is not configured to send DHCPINFORM message to the limited (all 1s) broadcast address.
2	←		DHCPOFFER	Sent if DHCP Discover message is received.
3	→		DHCPINFORM	Requesting P-CSCF Address(es)
4	←		DHCPACK	Including P-CSCF Address(es)
5	→		DNS NAPTR Query	UE configured to use specific Transport protocol on default ports, can skip steps 5 to 8 and go directly to step 9
6	←		DNS NAPTR Response	
7	→		DNS SRV Query	
8	←		DNS SRV Response	
9	→		DNS A Query	
10	←		DNS A Response	
11	→		REGISTER	UE sends initial registration for IMS services
12	←→		Continue with Annex C.2 or C.2a step 5	Execute the Generic test procedure Annex C.2 step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state

NOTE: The default messages contents in annex A are used with condition 'IMS security ' or 'GIBA' when applicable

Specific Message Contents:

DHCPDISCOVER (step 1)

Use the default message in annex B

DHCPOFFER (step 2)

Use the default message in annex B

DHCPINFORM (step 3)

Use the default message in annex B with the following exceptions

Field	Value/Remarks
Options	*
- code	53 (DHCP Message Type)
- len	1
-Type	2 (DHCP OFFER)
option-code - option-len	55 (Parameter Request List) Set to number of values requested for configuration parameters
Option code	120 (SIP Server Option) **
Option code	6(Domain Server) Optionally present

*NOTE 1:Other options may also be present

** NOTE 2: Other option codes may also be present and options can be in any order

DHCPACK (step 4)

Use the default message in annex B.2 with the following exceptions

Field	Value/Remarks
option-code - option-len -enc	120 (SIP Server option) Length of encoded server domain address +1 (for enc field) 0
Domain-address 1	SS P-CSCF server domain AddressRFC 3361[57]
option-code - option-len	6 (DNS option RFC 2132[49]))(Included only if requested in DHCP INFORM) 4
DNS Address	4 byte IPv4 address of DNS server

DNS NAPTR Query (step 5)

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	P-CSCF domain name received
QCLASS=	IN
QTYPE=	NAPTR

DNS NAPTR Response (step 6)

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in NAPTR Query
QCLASS=	IN
QTYPE=	NAPTR
NAPTR Records	NAPTR Records included for each Transport protocol (TLS, TCP, UDP) supported RFC 3263[50]

DNS SRV Query (step 7)

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Corresponding to the transport protocol selected by UE among those provided in DNS NAPTR Response
QCLASS=	IN
QTYPE=	SRV

DNS SRV Response (step 8)

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in SRV Query
QCLASS=	IN
QTYPE=	NAPTR
SRV Records	SRV Resource Record included providing the SS target server FQDN RFC 3263[50].

DNS A Query (step 9)

Case 1: steps 5 to 8 executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among provided in step 8 based on priority and weight RFC 2728[56]
QCLASS=	IN
QTYPE=	A

Case 2: steps 5 to 8 not executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among addresses provided in step 4.
QCLASS=	IN
QTYPE=	A

DNS A Response (step 10)

IE	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in SRV Query
QCLASS=	IN
QTYPE=	A
A or AAAA records	Includes resolved IP address(es).

7.2.5 Test requirements

1) In step 3, the UE shall initiate a P-CSCF discovery employing DHCP.

2) After step 4, the UE shall initiate a DNS query for domain address to IPv4 address translation.

3) In step 11, the UE shall send an initial REGISTER message using the discovered P-CSCF IPv4 address.

7.3 P-CSCF Discovery via DHCP – IPv4 (UE Requests P-CSCF discovery via PCO)

7.3.1 Definition

Test to verify that on not receiving P-CSCF Address(es) in PCO, UE will perform P-CSCF discovery procedure employing DHCP. The test case is applicable for IMS security or GIBA.

7.3.2 Conformance requirement

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure as specified in 3GPP TS 24.008 [8];

b) ensure that a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A] is available. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

…

c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

I. When using IPv4, employ the Dynamic Host Configuration Protocol (DHCP) RFC 2132 [20F], the DHCPv4 options for SIP servers RFC 3361 [35A], and RFC 3263 [27A] as described in subclause 9.2.1. When using IPv6, employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 [56C] as described in subclause 9.2.1.

II. Transfer P-CSCF address(es) within the PDP context activation procedure.

The UE shall indicate the request for a P-CSCF address to the GGSN within the Protocol Configuration Options information element of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message.

If the GGSN provides the UE with a list of P-CSCF IPv4 or IPv6 addresses in the ACTIVATE PDP CONTEXT ACCEPT message or ACTIVATE SECONDARY PDP CONTEXT ACCEPT message, the UE shall assume that the list is prioritised with the first address within the Protocol Configuration Options information element as the P-CSCF address with the highest priority.

...

The UE can freely select method I or II for P-CSCF discovery, if:

- the UE is in the home network; or

- the UE is roaming and the P-CSCF is to be discovered in the visited network .

In case method I is selected and several P-CSCF addresses or FQDNs are provided to the UE, the selection of P-CSCF address or FQDN shall be performed as indicated in RFC 3361 [35A] when using IPv4 or RFC 3319 [41] when using IPv6. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

NOTE 4: The UE decides whether the P-CSCF is to be discovered in the serving network or in the home network based on local configuration, e.g. whether the application on the UE is permitted to use local breakout.

If the UE is designed to use I above, but receives P-CSCF address(es) according to II, then the UE shall either ignore the received address(es), or use the address(es) in accordance with II, and not proceed with the DHCP request according to I.

When using IPv4, the UE may request a DNS Server IPv4 address(es) via RFC 2132 [20F] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

When using IPv6, the UE may request a DNS Server IPv6 address(es) via RFC 3315 [40] and RFC 3646 [56C] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

From 3GPP TR 23.981[35]:

The following mechanisms need to be evaluated for P-CSCF discovery in IPv4:

...

b) based on DHCP. Currently the specifications limit this to the IPv6 methods for DHCP. In order for this method to be used by an IPv4 UE, it needs to be identified how IPv4 DHCP is used to obtain the P-CSCF address. A solution that provides access independence would be that an IPv4 P-CSCF and IPv4 UE support configuration of the appropriate P-CSCF information via DHCPv4. In this solution, use of DHCP provides the UE with the fully qualified domain name of a P-CSCF and the address of a Domain Name Server (DNS) that is capable of resolving the P-CSCF name. When using DHCP/DNS procedure for P-CSCF discovery with IPv4 GPRS-access, the GGSN acts as DHCP Relay agent relaying DHCP messages between UE and the DHCP server. This is necessary to allow the UE to properly interoperate with the GGSN. This solution however requires that a UE supporting early IPv4 implementations would support DHCPv4.

Reference(s)

3GPP TS 24.229[10], clause B.2.2.1.

3GPP TR 23.981[35], clause 5.2.1.

7.3.3 Test purpose

To verify that the UE sends a correctly composed Activate PDP context request message requesting for P-CSCF address(es) to the GGSN within the Protocol Configuration Options IE.

On receiving Activate PDP Context accept not including P-CSCF address(es) in PCO, UE will initiate a P-CSCF discovery procedure employing DHCP/DNS.

7.3.4 Method of test

Initial conditions

The UE is in GMM-state "GMM-REGISTERED, normal service" with valid P-TMSI and CKSN. UE is not registered to IMS services, has not established PDP context. UE is not configured for using static P-CSCF address.

Related ICS/IXIT Statement(s)

UE Supports IPv4 (Yes/No)

UE capable of being configured to initiate P-CSCF Discovery via PCO (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

UE supports P-CSCF Discovery via PCO and DHCPv4(Yes/No)

Test procedure

1) UE is configured for requesting P-CSCF address(es) in Protocol Configuration Options IE in Activate PDP Context Request message. UE initiates an Activate PDP Context procedure.

2) SS Responds with an Activate PDP Context Accept message by not including P-CSCF Address(es). If a UE already knows DHCP server address, it goes to step 5. If UE sets flag "DNS Server Address Request" in PCO of PDP Context Request, DNS server address list is provided in PDP context Accept message.

3) If UE is configured to send DHCPINFORM message to the limited (all 1s) broadcast address, it goes to step 5. Otherwise, UE sends DHCPDISCOVER message locating a server.

4) SS responds by DHCPOFFER message.

5) UE sends DHCPINFORM message requesting for P-CSCF address(es) in options field.

6) SS responds by DHCPACK message providing the domain names of P-CSCF address(es) and giving a DNS server address.

7) UE initiates a DNS NAPTR query to select the transport protocol. UE"s configured to use specific Transport protocol on default ports, can skip steps 7 to 10 and go directly to step 11.

8) SS responds with NAPTR response.

9) UE initiates a DNS SRV query.

10) SS responds with SRV response.

11) UE initiates a DNS A or query.

12) SS responds with DNS A or response.

13) UE sends an initial REGISTER request.

14) Continue test execution with the Generic test procedure, Annex C.2, step 5.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		Activate PDP Context Request	UE sends this PDU by setting request for P-CSCF address(es) to the GGSN within the Protocol Configuration Options IE
2	←		Activate PDP Context Accept	SS Sends this response by not including P-CSCF address(es). If UE sets flag "DNS Server Address Request" in PCO of PDP Context Request, DNS server address list is provided in PDP context Accept message. If UE knows DHCP server address, goes to step 5.
3	→		DHCPDISCOVER	Optionally sent if UE is not configured to send DHCPINFORM message to the limited (all 1s) broadcast address.
4	←		DHCPOFFER	Sent if DHCP Discover message is received.
5	→		DHCPINFORM	Requesting P-CSCF Address(es)
6	←		DHCPACK	Including P-CSCF Address(es)
7	→		DNS NAPTR Query	UE"s configured to use specific Transport protocol on default ports, can skip steps 7 to 10 and go directly to step 11
8	←		DNS NAPTR Response	
9	→		DNS SRV Query	
10	←		DNS SRV Response	
11	→		DNS A or AAAA Query	
12	←		DNS A or AAAA Response	
13	→		REGISTER	UE sends initial registration for IMS services
14	←→		Continue with Annex C.2 or C.2a step 5	Execute the Generic test procedure Annex C.2 step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state

NOTE: The default messages contents in annex A are used with condition 'IMS security ' or 'GIBA' when applicable

Specific Message Contents:

Activate PDP Context Request (step 1)

IE	Value/Remarks
Protocol Configuration options - Additional Parameters -- container 1 Identifier -- Container 1 Length	 0001H (P-CSCF Address Request) 0 bytes

Activate PDP Context Accept (step 2)

IE	Value/Remarks
Protocol Configuration options - Additional Parameters -- container 1 Identifier -- Container 1 Length -- Container 1 contents	Present only if "DNS Server Address Request" received in Request message 0003H (DNS Address) 16 bytes IPV4 address of SS DNS server encoded as per 3GPP TR 23.981[35]

DHCPDISCOVER (step 3)

Use the default message in annex B.

DHCPOFFER (step 4)

Use the default message in annex B.

DHCPINFORM (step 5)

Use the default message in annex B with the following exceptions:

Field	Value/Remarks
Options - code - len -Type	* 53 (DHCP Message Type) 1 2 (DHCP OFFER)
option-code - option-len	55 (Parameter Request List) Set to number of values requested for configuration parameters
Option code	120 (SIP Server Option) **
Option code	6(Domain Server) Optionally present

*NOTE 1:Other options may also be present.

** NOTE 2: Other option codes may also be present and options can be in any order.

DHCPACK (step 6)

Use the default message in annex B with the following exceptions:

Field	Value/Remarks
option-code - option-len -enc	120 (SIP Server option) Length of encoded server domain address +1 (for enc field) 0
Domain-address 1	SS P-CSCF server domain AddressRFC 3361[57]
option-code - option-len	6 (DNS option RFC 2132[49]) (Included only if requested in DHCP INFORM) 4
DNS Address	4 byte IPv4 address of DNS server

DNS NAPTR Query (step 7)

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	P-CSCF domain name received
QCLASS=	IN
QTYPE=	NAPTR

DNS NAPTR Response (step 8)

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in NAPTR Query
QCLASS=	IN
QTYPE=	NAPTR
NAPTR Records	NAPTR Records included for each Transport protocol (TLS, TCP, UDP) supported RFC 3263[50]

DNS SRV Query (step 9)

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Corresponding to the transport protocol selected by UE among those provided in DNS NAPTR Response
QCLASS=	IN
QTYPE=	SRV

DNS SRV Response (step 10)

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in SRV Query
QCLASS=	IN
QTYPE=	NAPTR
SRV Records	SRV Resource Record included providing the SS target server FQDN RFC 3263[50].

DNS A Query (step 11)

Case 1: steps 7 to 10 executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among provided in step 8 based on priority and weight RFC 2728[56]
QCLASS=	IN
QTYPE=	A

Case 2: steps 7 to 10 not executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among addresses provided in step 6.
QCLASS=	IN
QTYPE=	A

DNS A Response (step 12)

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in SRV Query
QCLASS=	IN
QTYPE=	A
A records	Includes resolved IP address(es).

7.3.5 Test requirements

1) In step 1, the UE shall set the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE.

2) After step 2, the UE shall initiate a P-CSCF discovery employing DHCP.

3) In step 3, if the UE has no knowledge of a DHCP server address and is not configured to send a DHCPINFORM message to the limited (all 1s) broadcast address then it shall send a DHCPDISCOVER message.

4) In step 5, the UE shall send a DHCPRequest message, including options filed with option code 120.

5) After step 6, the UE shall initiate a DNS query.

6) In step 13, the UE shall send an initial REGISTER message using the discovered P-CSCF IPv4 address.

7.4 P-CSCF Discovery by DHCP - IPv6

7.4.1 Definition

Test to verify that UE will perform P-CSCF discovery procedure employing DHCP. The test case is applicable for IMS security or GIBA.

7.4.2 Conformance requirement

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure as specified in 3GPP TS 24.008 [8];

b) ensure that a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A] is available. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

…

c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

I. When using IPv4, employ the Dynamic Host Configuration Protocol (DHCP) RFC 2132 [20F], the DHCPv4 options for SIP servers RFC 3361 [35A], and RFC 3263 [27A] as described in subclause 9.2.1. When using IPv6, employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 [56C] as described in subclause 9.2.1.

II. …

The UE shall indicate the request for a P-CSCF address to the GGSN within the Protocol Configuration The UE can freely select method I or II for P-CSCF discovery, if:

- the UE is in the home network; or

- the UE is roaming and the P-CSCF is to be discovered in the visited network .

In case method I is selected and several P-CSCF addresses or FQDNs are provided to the UE, the selection of P-CSCF address or FQDN shall be performed as indicated in RFC 3361 [35A] when using IPv4 or RFC 3319 [41] when using IPv6. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

NOTE 4: The UE decides whether the P-CSCF is to be discovered in the serving network or in the home network based on local configuration, e.g. whether the application on the UE is permitted to use local breakout.

If the UE is designed to use I above, but receives P-CSCF address(es) according to II, then the UE shall either ignore the received address(es), or use the address(es) in accordance with II, and not proceed with the DHCP request according to I.

When using IPv4, the UE may request a DNS Server IPv4 address(es) via RFC 2132 [20F] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

When using IPv6, the UE may request a DNS Server IPv6 address(es) via RFC 3315 [40] and RFC 3646 [56C] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

The encoding of the request and response for IPv4 or IPv6 address(es) for DNS server(s) and list of P-CSCF address(es) within the Protocol Configuration Options information element is described in 3GPP TS 24.008 [8].

.

Reference(s)

3GPP TS 24.229[10], clause B.2.2.1,.

7.4.3 Test purpose

To verify UE shall initiate and successfully complete a P-CSCF discovery procedure via DHCP when P-CSCF address is not provided as part of PDP Context Activation procedure.

7.4.4 Method of test

Initial conditions

The UE is in GMM-state "GMM-REGISTERED, normal service" with valid P-TMSI and CKSN. UE is not registered to IMS services. UE has established a PDP context. UE has not received P-CSCF address(es) during PDP context establishment. If UE sets flag "DNS Server Address Request" in PCO of PDP Context Request, DNS server address list is provided in PDP Context Accept message.

Related ICS/IXIT Statement(s)

UE Supports IPv6 (Yes/No)

UE capable of being configured to initiate P-CSCF Discovery via DHCPv6 (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Test procedure

1. UE may send DHCP SOLICIT message locating a server. If UE is configured to send Information-Request to "All_DHCP_Relay_Agents_and_Servers" multicast address, test case starts at step 3.
2. SS responds with DHCP ADVERTISE message. If UE requested for domain names or both domain names and IP address(es), SS will include P-CSCF server domain names. If UE requested for IP address only, SS includes IP address(es) of P-CSCF servers. If UE Requested for DNS Server Address, it is provided. If P-CSCF IP addresses are included go to step 11, else go to step 5
3. UE sends DHCP Query requesting either IP address(es) of P-CSCF server(s) or domain names of P-CSCF server(s) and DNS Server.
4. SS responds by DHCP Reply message. If UE requested for domain names or both domain names and IP address(es), SS will include P-CSCF server domain names. If UE requested for IP address only, SS includes IP address(es) of P-CSCF servers. If UE Requested for DNS Server Address, it is provided. If P-CSCF IP addresses are included go to step 11.
5. UE initiates a DNS NAPTR query to select the transport protocol. UE"s configured to use specific Transport protocol on default ports, can skip steps 5 to 8 and go directly to step 9.
6. SS responds with NAPTR response.
7. UE initiates a DNS SRV query.
8. SS responds with SRV response.

9. UE initiates a DNS AAAA query.
10. SS responds with DNS AAAA response.
11. UE sends an initial REGISTER request.
12. Continue test execution with the Generic test procedure, Annex C.2, step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		DHCP SOLICIT	Optional message
2	←		DHCP ADVERTISE	Sent if DHCP Solicit message is received. Including P-CSCF Address(es). If P-CSCF IP addresses are included go to step 11, else go to step 5
3	→		DHCP Information-Request	Requesting P-CSCF Address(es)*
4	←		DHCP Reply	Including P-CSCF Address(es). If P-CSCF IP addresses are included go to step 11.
5	→		DNS NAPTR Query	UE"s configured to use specific Transport protocol on default ports, can skip steps 5 to 8 and go directly to step 9
6	←		DNS NAPTR Response	
7	→		DNS SRV Query	
8	←		DNS SRV Response	
9	→		DNS AAAA Query	
10	←		DNS AAAA Response	
11	→		REGISTER	UE sends initial registration for IMS services
12	←→		Continue with Annex C.2 or C.2a step 5	Execute the Generic test procedure Annex C.2 step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state

* NOTE: UE may request all options in one Information Request or send multiple Information Requests. If UE opts for multiple Information Request transmissions, SS transmits accordingly multiple Reply messages including corresponding requested options.

NOTE: The default messages contents in annex A are used with condition 'IMS security ' or 'GIBA' when applicable

Specific Message Contents:

Step 1: DHCP SOLICIT*

Use the default message in annex B.1 with the following exceptions

Options	Value/Remarks
option-code	OPTION_ORO (6)
- option-len	2 times number of requested options
-requested-option-code-1	OPTION_SIP_SERVER_D (21) OR OPTION_SIP_SERVER_A (22)
- requested-option-code-2	OPTION_DNS_SERVERS (23)
- requested-option-code-3	OPTION_DOMAIN_LIST (24)

*NOTE: Options can be optionally present and option codes can be in any order

**NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 2: DHCP ADVERTISE

Use the default message in annex B.1 with the following exceptions

NOTE: Options are included only if corresponding Requests are received.

Case 1: (OPTION_SIP_SERVER_D (21)) or both (OPTION_SIP_SERVER_D (21) and OPTION_SIP_SERVER_A (22)) and OPTION_DOMAIN_LIST(24) or OPTION_DNS_SERVERS (23) received in step 1

Options	Value/Remarks
option-code - option-len	OPTION_SIP_SERVER_D (21) Length of encoded domain address RFC 3319[51]
Domain-address 1	SS P-CSCF server domain address RFC 3319[51]
option-code - option-len Domain-address 1	OPTION_DNS_SERVERS (23) Length of encoded DNS server address RFC 3646[48] SS DNS server IPv6 address RFC 3646[48]
option-code - option-len	OPTION_DOMAIN_LIST (24) Length of Domain search list
searchlist	List of Domain Names encoded as per RFC 1035[52]

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Case 2: OPTION_SIP_SERVER_A (22) received in step 1

Options	Value/Remarks
option-code - option-len	OPTION_SIP_SERVER_A (22) 128
Domain-address 1	IPv6 address of SS P-CSCF Server
option-code - option-len	OPTION_DNS_SERVERS (23) Length of encoded DNS server address RFC 3646[48]
Domain-address 1	SS DNS server IPv6 address RFC 3646[48]
option-code - option-len	OPTION_DOMAIN_LIST (24) Length of Domain search list
searchlist	List of Domain Names encoded as per RFC 1035[52]

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 3: DHCP Information-Request

Use the default message in annex B.1 with the following exceptions

Options	Value/Remarks
option-code - option-len - requested-option-code-1 - requested-option-code-2 - requested-option-code-3	OPTION_ORO (6) 2 * number of requested options OPTION_SIP_SERVER_D (21) OR OPTION_SIP_SERVER_A (22) OPTION_DNS_SERVERS (23)(Optional) OPTION_DOMAIN_LIST (24) (Optional)

NOTE: All options can be either received in one message or multiple messages. If more than one option codes present they can be in any order.

**NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 4: DHCP Reply

Use the default message in annex B.1 with the following exceptions

NOTE: Options are included only if corresponding Requests are received.

Case 1: OPTION_SIP_SERVER_D (21)) or both (OPTION_SIP_SERVER_D (21) and OPTION_SIP_SERVER_A (22)) and OPTION_DOMAIN_LIST(24) or OPTION_DNS_SERVERS (23) received in step 3

Options	Value/Remarks
option-code - option-len	OPTION_SIP_SERVER_D (21) Length of encoded domain address RFC 3319[51]
Domain-address 1	SS P-CSCF server domain Address RFC 3319[51]
option-code - option-len Domain-address 1	OPTION_DNS_SERVERS (23) Length of encoded DNS server address RFC 3646[48] SS DNS server IPv6 address RFC 3646[48]
option-code - option-len	OPTION_DOMAIN_LIST (24) Length of Domain search list
searchlist	List of Domain Names encoded as per RFC 1035[52]

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Case 2: OPTION_SIP_SERVER_A (22) received in step 3

Options	Value/Remarks
option-code - option-len	OPTION_SIP_SERVER_A (22) 128
Domain-address 1	IPv6 address of SS P-CSCF Server
option-code - option-len	OPTION_DNS_SERVERS (23) Length of encoded DNS server address RFC 3646[48]
Domain-address 1	SS DNS server IPv6 address RFC 3646[48]
option-code - option-len	OPTION_DOMAIN_LIST (24) Length of Domain search list
searchlist	List of Domain Names encoded as per RFC 1035 [52]

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 5: DNS NAPTR Query

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	P-CSCF domain name received
QCLASS=	IN
QTYPE=	NAPTR

Step 6: DNS NAPTR Response

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in NAPTR Query
QCLASS=	IN
QTYPE=	NAPTR
NAPTR Records	NAPTR Records included for each Transport protocol (TLS, TCP, UDP) supported RFC 3263[50]

Step 7: DNS SRV Query

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Corresponding to the transport protocol selected by UE among those provided in DNS NAPTR Response
QCLASS=	IN
QTYPE=	SRV

Step 8: DNS SRV Response

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in SRV Query
QCLASS=	IN
QTYPE=	SRV
SRV Records	SRV Resource Record included providing the SS target server FQDN RFC 3263[50].

Step 9: DNS AAAA Query

Case 1: steps 5 to 8 executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among provided in step 8 based on priority and weight RFC 2728[56]
QCLASS=	IN
QTYPE=	AAAA

Case 2: steps 5 to 8 not executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among addresses provided in step 2 or 4.
QCLASS=	IN
QTYPE=	AAAA

Step 10: DNS AAAA Response

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in AAAA Query
QCLASS=	IN
QTYPE=	AAAA
AAAA records	Includes resolved IP address(es).

7.4.5 Test requirements

1. In step 1, the UE shall initiate a P-CSCF discovery employing DHCP.
2. After steps 2 and 4, if a P-CSCF IPv6 address is received then the UE will consider the P-CSCF discovery procedure successful, else the UE will initiate a DNS query for domain address to IPv6 address translation.
3. In step 11, the UE shall send an initial REGISTER message using the discovered P-CSCF address.

7.5 P-CSCF Discovery by DHCP-IPv6 (UE Requests P-CSCF discovery by PCO)

7.5.1 Definition

Test to verify that on not receiving P-CSCF Address(es) in PCO, will perform P-CSCF discovery procedure employing DHCP. The test case is applicable for IMS security or GIBA.

7.5.2 Conformance requirement

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure as specified in 3GPP TS 24.008 [8]re;

b) ensure that a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A] is available. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

…

c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

I. When using IPv4, employ the Dynamic Host Configuration Protocol (DHCP) RFC 2132 [20F], the DHCPv4 options for SIP servers RFC 3361 [35A], and RFC 3263 [27A] as described in subclause 9.2.1. When using IPv6, employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 [56C] as described in subclause 9.2.1.

II. Transfer P-CSCF address(es) within the PDP context activation procedure.

The UE shall indicate the request for a P-CSCF address to the GGSN within the Protocol Configuration Options information element of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message.

If the GGSN provides the UE with a list of P-CSCF IPv4 or IPv6 addresses in the ACTIVATE PDP CONTEXT ACCEPT message or ACTIVATE SECONDARY PDP CONTEXT ACCEPT message, the UE shall assume that the list is prioritised with the first address within the Protocol Configuration Options information element as the P-CSCF address with the highest priority.

...

The UE can freely select method I or II for P-CSCF discovery, if:

- the UE is in the home network; or

- the UE is roaming and the P-CSCF is to be discovered in the visited network .

In case method I is selected and several P-CSCF addresses or FQDNs are provided to the UE, the selection of P-CSCF address or FQDN shall be performed as indicated in RFC 3361 [35A] when using IPv4 or RFC 3319 [41] when using IPv6. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

NOTE 4: The UE decides whether the P-CSCF is to be discovered in the serving network or in the home network based on local configuration, e.g. whether the application on the UE is permitted to use local breakout.

If the UE is designed to use I above, but receives P-CSCF address(es) according to II, then the UE shall either ignore the received address(es), or use the address(es) in accordance with II, and not proceed with the DHCP request according to I.

When using IPv4, the UE may request a DNS Server IPv4 address(es) via RFC 2132 [20F] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

When using IPv6, the UE may request a DNS Server IPv6 address(es) via RFC 3315 [40] and RFC 3646 [56C] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

The encoding of the request and response for IPv4 or IPv6 address(es) for DNS server(s) and list of P-CSCF address(es) within the Protocol Configuration Options information element is described in 3GPP TS 24.008 [8].

Reference(s)

3GPP TS 24.229[10], clause B.2.2.1,.

7.5.3 Test purpose

To verify that the UE sends a correctly composed Activate PDP context requesting for P-CSCF address(es) to the GGSN within the Protocol Configuration Options IE.

On receiving Activate PDP Context accept not including P-CSCF address(es) in PCO IE, will initiate a P-CSCF discovery procedure employing DHCP.

7.5.4 Method of test

Initial conditions

The UE is in GMM-state "GMM-REGISTERED, normal service" with valid P-TMSI and CKSN. UE is not registered to IMS services, has not established PDP context.

Related ICS/IXIT Statement(s)

UE Supports IPv6 (Yes/No)

UE capable of being configured to initiate P-CSCF Discovery via PCO (Yes/No)

UE supports P-CSCF Discovery via PCO and DHCPv6(Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Test procedure

1. UE is configured for requesting P-CSCF address(es) in Protocol Configuration Options IE in Activate PDP Context Request message. UE initiates an Activate PDP Context procedure.
2. SS Responds with an Activate PDP Context Accept message by not including P-CSCF address(es). If UE sets flag "DNS Server Address Request" in PCO of PDP Context Request, DNS server address list is provided in PDP Context Accept message.
3. UE may send DHCP Solicit message locating a server. If UE is configured to send Information-Request to "All_DHCP_Relay_Agents_and_Servers" multicast address, go to step 5.
4. SS responds by Advertise message. If UE requested for domain names or both domain names and IP address(es), SS will include P-CSCF server domain names. If UE requested for IP address only, SS includes IP address(es) of P-CSCF servers. If UE Requested for DNS Server Address, it is provided. If P-CSCF IP addresses are included go to step 13 else go to step 7.
5. UE sends DHCP Information-Request Query requesting either IP address(es) of P-CSCF server(s) or domain names of P-CSCF server(s) and DNS Server.
6. SS responds by DHCP Reply message. . If UE requested for domain names or both domain names and IP address(es), SS will include P-CSCF server domain names. If UE requested for IP address only, SS includes IP address(es) of P-CSCF servers. If UE Requested for DNS Server Address, it is provided. If P-CSCF IP addresses are included go to step 13.
7. UE initiates a DNS NAPTR query to select the transport protocol. UE"s configured to use specific Transport protocol on default ports, can skip steps 7 to 10 and go directly to step 11.
8. SS responds with NAPTR response.
9. UE initiates a DNS SRV query.

10. SS responds with SRV response.
11. UE initiates a DNS AAAA query.
12. SS responds with DNS AAAA response.
13. UE sends an initial REGISTER request.
14. Continue test execution with the Generic test procedure, Annex C.2, step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		Activate PDP Context Request	UE sends this PDU by setting request for P-CSCF address(es) to the GGSN within the Protocol Configuration Options IE
2	←		Activate PDP Context Accept	SS Sends this response by not including P-CSCF address(es). If UE sets flag "DNS Server Address Request" in PCO of PDP Context Request, DNS server address list is provided.
3	→		DHCP SOLICIT	Optional message
4	→		DHCP ADVERTISE	Sent if DHCP Solicit message is received. Including P-CSCF Address(es). If P-CSCF IP addresses are included go to step 13 else go to step 7
5	→		DHCP Information-Request	Requesting P-CSCF Address(es)*
6	←		DHCP Reply	Including P-CSCF Address(es). If P-CSCF IP addresses are included go to step 13.
7	→		DNS NAPTR Query	UE"s configured to use specific Transport protocol on default ports, can skip steps 7 to 10 and go directly to step 11
8	←		DNS NAPTR Response	
9	→		DNS SRV Query	
10	←		DNS SRV Response	
11	→		DNS AAAA Query	
12	←		DNS AAAA Response	
13	→		REGISTER	UE sends initial registration for IMS services
14	←→		Continue with Annex C.2 or C.2a step 5	Execute the Generic test procedure Annex C.2 step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state

* NOTE: UE may request all options in one Information Request or send multiple Information Requests. If UE opts for multiple Information Request transmissions, SS transmits accordingly multiple Reply messages including corresponding requested options.

NOTE: The default messages contents in annex A are used with condition 'IMS security ' or 'GIBA' when applicable

Specific Message Contents:

Step 1: Activate PDP Context Request

Options	Value/Remarks
Protocol Configuration options	
- Additional Parameters	
-- container 1 Identifier	0001H (P-CSCF Address Request)
-- Container 1 Length	0 bytes
-- container 2 Identifier	0003H (DNS Server Address Request) (Optionally present)
-- Container 2 Length	0 bytes

Step 2: Activate PDP Context Accept

Options	Value/Remarks
Protocol Configuration options - Additional Parameters -- container 1 Identifier -- Container 1 Length -- Container 1 contents	(Included if "DNS Server Address Request" is received) 0003H (DNS Address) 16 bytes IPV6 address of SS DNS Server

Step 3: DHCP SOLICIT*

Use the default message in annex B.1 with the following exceptions

Options	Value/Remarks
option-code - option-len - requested-option-code-1 - requested-option-code-2 - requested-option-code-3	OPTION_ORO (6) 2 times number of requested options OPTION_SIP_SERVER_D (21) OR OPTION_SIP_SERVER_A (22) OPTION_DNS_SERVERS (23) OPTION_DOMAIN_LIST (24)

*NOTE: Options can be optionally present and option codes can be in any order

**NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 4: DHCP ADVERTISE

Use the default message in annex B.1 with the following exceptions

NOTE: Options are included only if corresponding Requests are received.

Case 1: OPTION_SIP_SERVER_D (21) or both (OPTION_SIP_SERVER_D (21) and OPTION_SIP_SERVER_A (22)) and OPTION_DOMAIN_LIST(24) or OPTION_DNS_SERVERS (23) received in step 3

Options	Value/Remarks
option-code - option-len Domain-address 1	OPTION_SIP_SERVER_D (21) Length of encoded domain address RFC 3319[51] SS P-CSCF server domain Address RFC 3319[51]
option-code - option-len Domain-address 1	OPTION_DNS_SERVERS (23) Length of encoded DNS server address RFC 3646[48] SS DNS server IPv6 address RFC 3646[48]
option-code - option-len	OPTION_DOMAIN_LIST (24) Length of Domain search list
searchlist	List of Domain Names encoded as per RFC 1035[52]

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Case 2: OPTION_SIP_SERVER_A (22) received in step 3

Options	Value/Remarks
option-code - option-len Domain-address 1	OPTION_SIP_SERVER_A (22) 128 IPv6 address of SS P-CSCF Server
option-code - option-len Domain-address 1	OPTION_DNS_SERVERS (23) Length of encoded DNS server address RFC 3646[48] SS DNS server IPv6 address RFC 3646[48]
option-code - option-len searchlist	OPTION_DOMAIN_LIST (24) Length of Domain search list List of Domain Names encoded as per RFC 1035 [52]

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 5: DHCP Information-Request

Use the default message in annex B.1 with the following exceptions

Options	Value/Remarks
option-code	OPTION_ORO (6)
- option-len	2 * number of requested options
-requested-option-code-1	OPTION_SIP_SERVER_D (21) OR OPTION_SIP_SERVER_A (22)
- requested-option-code-2	OPTION_DNS_SERVERS (23)(Optional)
- requested-option-code-3	OPTION_DOMAIN_LIST (24) (Optional)

NOTE: All options can be either received in one message or multiple messages. If more than one option codes present they can be in any order.

**NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 6: DHCP Reply

Use the default message in annex B.1 with the following exceptions

NOTE: Options are included only if corresponding Requests are received.

Case 1: (OPTION_SIP_SERVER_D (21)) or both (OPTION_SIP_SERVER_D (21) and OPTION_SIP_SERVER_A (22)) and OPTION_DOMAIN_LIST(24) or OPTION_DNS_SERVERS (23) received in step 5

Options	Value/Remarks
option-code	OPTION_SIP_SERVER_D (21)
- option-len	Length of encoded domain address RFC 3319[51]
Domain-address 1	SS P-CSCF server domain Address RFC 3319[51]
option-code	OPTION_DNS_SERVERS (23)
- option-len	Length of encoded DNS server address RFC 3646[48]
Domain-address 1	SS DNS server IPv6 address RFC 3646[48]
option-code	OPTION_DOMAIN_LIST (24)
- option-len	Length of Domain search list
searchlist	List of Domain Names encoded as per RFC 1035[52]

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Case 2: OPTION_SIP_SERVER_A (22) received in step 5

Options	Value/Remarks
option-code	OPTION_SIP_SERVER_A (22)
- option-len	128
Domain-address 1	IPv6 address of SS P-CSCF Server
option-code	OPTION_DNS_SERVERS (23)
- option-len	Length of encoded DNS server address RFC 3646[48]
Domain-address 1	SS DNS server IPv6 address RFC 3646[48]
option-code	OPTION_DOMAIN_LIST (24)
- option-len	Length of Domain search list
searchlist	List of Domain Names encoded as per RFC 1035 [52]

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 7: DNS NAPTR Query

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	P-CSCF domain name received
QCLASS=	IN
QTYPE=	NAPTR

Step 8: DNS NAPTR Response

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in NAPTR Query
QCLASS=	IN
QTYPE=	NAPTR
NAPTR Records	NAPTR Records included for each Transport protocol (TLS, TCP, UDP) supported RFC 3263[50]

Step 9: DNS SRV Query

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Corresponding to the transport protocol selected by UE among those provided in DNS NAPTR Response
QCLASS=	IN
QTYPE=	SRV

Step 10: DNS SRV Response

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in SRV Query
QCLASS=	IN
QTYPE=	SRV
SRV Records	SRV Resource Record included providing the SS target server FQDN RFC 3263[50].

Step 11: DNS AAAA Query

Case 1: steps 7 to 10 executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among provided in step 10 based on priority and weight RFC 2728[56]
QCLASS=	IN
QTYPE=	AAAA

Case 2: steps 7 to 10 not executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among addresses provided in step 4 or 6.
QCLASS=	IN
QTYPE=	AAAA

Step 12: DNS AAAA Response

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in AAAA Query
QCLASS=	IN
QTYPE=	AAAA
AAAA records	Includes resolved IP address(es).

7.5.5 Test requirements

1. In step 1, the UE shall set the IM CN Subsystem Signalling Flag to the GGSN within the Protocol Configuration Options IE.

2. After step 2, the UE shall initiate a P-CSCF discovery employing DHCP.

3. After step 6, if a P-CSCF IPv6 address is received then the UE will consider the P-CSCF discovery procedure successful, else the UE will initiate a DNS query for domain address to IPv6 address translation.

4. In step 13, the UE shall send an initial REGISTER message using the discovered P-CSCF address.

7.6 P-CSCF Discovery by DHCP – IPv6 (UE does not Request P-CSCF discovery by PCO, SS includes P-CSCF Address(es) in PCO)

7.6.1 Definition

Test to verify that on not receiving P-CSCF Address(es) in PCO, will perform P-CSCF discovery procedure employing DHCP. The test case is applicable for IMS security or GIBA.

7.6.2 Conformance requirement

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure as specified in 3GPP TS 24.008 [8];

b) ensure that a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A] is available. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

…

c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

I. When using IPv4, employ the Dynamic Host Configuration Protocol (DHCP) RFC 2132 [20F], the DHCPv4 options for SIP servers RFC 3361 [35A], and RFC 3263 [27A] as described in subclause 9.2.1. When using IPv6, employ Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [40], the DHCPv6 options for SIP servers RFC 3319 [41] and DHCPv6 options for Domain Name Servers (DNS) RFC 3646 [56C] as described in subclause 9.2.1.

II. Transfer P-CSCF address(es) within the PDP context activation procedure.

The UE shall indicate the request for a P-CSCF address to the GGSN within the Protocol Configuration Options information element of the ACTIVATE PDP CONTEXT REQUEST message or ACTIVATE SECONDARY PDP CONTEXT REQUEST message.

If the GGSN provides the UE with a list of P-CSCF IPv4 or IPv6 addresses in the ACTIVATE PDP CONTEXT ACCEPT message or ACTIVATE SECONDARY PDP CONTEXT ACCEPT message, the UE shall assume that the list is prioritised with the first address within the Protocol Configuration Options information element as the P-CSCF address with the highest priority.

...

The UE can freely select method I or II for P-CSCF discovery, if:

- the UE is in the home network; or

- the UE is roaming and the P-CSCF is to be discovered in the visited network .

In case method I is selected and several P-CSCF addresses or FQDNs are provided to the UE, the selection of P-CSCF address or FQDN shall be performed as indicated in RFC 3361 [35A] when using IPv4 or RFC 3319 [41] when using IPv6. If sufficient information for P-CSCF address selection is not available, selection of the P-CSCF address by the UE is implementation specific.

NOTE 4: The UE decides whether the P-CSCF is to be discovered in the serving network or in the home network based on local configuration, e.g. whether the application on the UE is permitted to use local breakout.

If the UE is designed to use I above, but receives P-CSCF address(es) according to II, then the UE shall either ignore the received address(es), or use the address(es) in accordance with II, and not proceed with the DHCP request according to I.

When using IPv4, the UE may request a DNS Server IPv4 address(es) via RFC 2132 [20F] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

When using IPv6, the UE may request a DNS Server IPv6 address(es) via RFC 3315 [40] and RFC 3646 [56C] or by the Protocol Configuration Options information element when activating a PDP context according to 3GPP TS 27.060 [10A].

The encoding of the request and response for IPv4 or IPv6 address(es) for DNS server(s) and list of P-CSCF address(es) within the Protocol Configuration Options information element is described in 3GPP TS 24.008 [8].

Reference(s)

3GPP TS 24.229[10], clause B.2.2.1,.

7.6.3 Test purpose

To verify that a UE, which has not requested for P-CSCF address in PDP context activate message, receives P-CSCF address, may accept the P-CSCF address or ignore it and hence initiate P-CSCF discovery by DHCP.

7.6.4 Method of test

Initial conditions

The UE is in GMM-state "GMM-REGISTERED, normal service" with valid P-TMSI and CKSN. UE is not registered to IMS services, has not established PDP context.

Related ICS/IXIT Statement(s)

UE Supports IPv6 (Yes/No)

UE capable of being configured to initiate P-CSCF Discovery via DHCPv6 (Yes/No)

UE supports P-CSCF Discovery via PCO and DHCPv6 (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Test procedure

1. UE is configured for not requesting P-CSCF addresses in PCO.
2. SS Responds with an Activate PDP Context Accept message by including P-CSCF Address(es). UE can either assume P-CSCF procedure to be complete or neglect the P-CSCF address(es) in PDP context Accept. Test Ends if UE assumes P-CSCF procedure to be complete.
3. UE may send Solicit message locating a server. If UE is configured to send Information-Request to "All_DHCP_Relay_Agents_and_Servers" multicast address, go to step 5.
4. SS responds by Advertise message. If UE requested for domain names or both domain names and IP address(es), SS will include P-CSCF server domain names. If UE requested for IP address only, SS includes IP address(es) of P-CSCF servers. If UE Requested for DNS Server Address, it is provided. If P-CSCF IP addresses are included go to step 13, else go to step 7.
5. UE sends DHCP Information-Request Query requesting either IP address(es) of P-CSCF server(s) or domain names of P-CSCF server(s) and DNS Server.
6. SS responds by DHCP Reply message. If UE requested for domain names or both domain names and IP address(es), SS will include P-CSCF server domain names. If UE requested for IP address only, SS includes IP address(es) of P-CSCF servers. If UE Requested for DNS Server Address, it is provided. If P-CSCF IP addresses are included go to step 13.
7. UE initiates a DNS NAPTR query to select the transport protocol. UE"s configured to use specific Transport protocol on default ports, can skip steps 7 to 10 and go directly to step 11.
8. SS responds with NAPTR response.
9. UE initiates a DNS SRV query.
10. SS responds with SRV response.
11. UE initiates a DNS AAAA query.
12. SS responds with DNS AAAA response.
13. UE sends an initial REGISTER request.
14. Continue test execution with the Generic test procedure, Annex C.2, step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		Activate PDP Context Request	UE sends this PDU not requesting for P-CSCF address(es)
2	←		Activate PDP Context Accept	SS Sends this response including P-CSCF Address(es). UE shall either ignore the received address, or use the address. If UE uses address, go to step 13.
3	→		DHCP SOLICIT	Optional message
4	←		DHCP ADVERTISE	Sent if DHCP Solicit message is received. Including P-CSCF Address(es). If P-CSCF IP addresses are included go to step 13, else go to step 7
5	→		DHCP Information-Request	Requesting P-CSCF Address(es)*
6	←		DHCP Reply	Including P-CSCF Address(es). If P-CSCF IP addresses are included go to step 13.
7	→		DNS NAPTR Query	UE"s configured to use specific Transport protocol on default ports, can skip steps 7 to 10 and go directly to step 11
8	←		DNS NAPTR Response	
9	→		DNS SRV Query	
10	←		DNS SRV Response	
11	→		DNS AAAA Query	
12	←		DNS AAAA Response	
13	→		REGISTER	UE sends initial registration for IMS services
14	←→		Continue with Annex C.2 or C.2a step 5	Execute the Generic test procedure Annex C.2 step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state

* NOTE: UE may request all options in one Information Request or send multiple Information Requests. If UE opts for multiple Information Request transmissions, SS transmits accordingly multiple Reply messages including corresponding requested options.

NOTE: The default messages contents in annex A are used with condition 'IMS security ' or 'GIBA' when applicable

Specific Message Contents:

Step 2: Activate PDP Context Accept

Options	Value/Remarks
Protocol Configuration options	
- Additional Parameters	
-- container 1 Identifier	0001H (P-CSCF Address)
-- Container 1 Length	16 bytes
-- Container 1 contents	IPV6 address of SS
-- container 2 Identifier	0003H (DNS Address)
-- Container 2 Length	16 bytes
-- Container 2 contents	IPV6 address of SS DNS Server

Step 3: DHCP SOLICIT*

Use the default message in annex B.1 with the following exceptions

Options	Value/Remarks
option-code	OPTION_ORO (6)
- option-len	2 times number of requested options
-requested-option-code-1	OPTION_SIP_SERVER_D (21) OR OPTION_SIP_SERVER_A (22)
- requested-option-code-2	OPTION_DNS_SERVERS (23)
- requested-option-code-3	OPTION_DOMAIN_LIST (24)

*NOTE: Options can be optionally present and option codes can be in any order

**NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 4: DHCP ADVERTISE

Use the default message in annex B.1 with the following exceptions

NOTE: Options are included only if corresponding Requests are received.

Case 1: (OPTION_SIP_SERVER_D (21)) or both (OPTION_SIP_SERVER_D (21) and OPTION_SIP_SERVER_A (22)) and OPTION_DOMAIN_LIST(24) or OPTION_DNS_SERVERS (23) received in step 3

Options	Value/Remarks
option-code	OPTION_SIP_SERVER_D (21)
- option-len	Length of encoded domain address RFC 3319[51]
Domain-address 1	SS P-CSCF server domain Address RFC 3319[51]
option-code	OPTION_DNS_SERVERS (23)
- option-len	Length of encoded DNS server address RFC 3646[48]
Domain-address 1	SS DNS server IPv6 address RFC 3646[48]
option-code	OPTION_DOMAIN_LIST (24)
- option-len	Length of Domain search list
searchlist	List of Domain Names encoded as per RFC 1035 [52]

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Case 2: OPTION_SIP_SERVER_A (22) received in step 3

Options	Value/Remarks
option-code	OPTION_SIP_SERVER_A (22)
- option-len	128
Domain-address 1	IPv6 address of SS P-CSCF Server
option-code	OPTION_DNS_SERVERS (23)
- option-len	Length of encoded DNS server address RFC 3646[48]
Domain-address 1	SS DNS server IPv6 address RFC 3646[48]
option-code	OPTION_DOMAIN_LIST (24)
- option-len	Length of Domain search list
searchlist	List of Domain Names encoded as per RFC 1035 [52]

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 5: DHCP Information-Request

Use the default message in annex B.1 with the following exceptions

Options	Value/Remarks
option-code	OPTION_ORO (6)
- option-len	2 * number of requested options
-requested-option-code-1	OPTION_SIP_SERVER_D (21) OR OPTION_SIP_SERVER_A (22)
- requested-option-code-2	OPTION_DNS_SERVERS (23)(Optional)
- requested-option-code-3	OPTION_DOMAIN_LIST (24) (Optional)

NOTE: All options can be either received in one message or multiple messages. If more than one option codes present they can be in any order.

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 6: DHCP Reply

Use the default message in annex B.1 with the following exceptions

NOTE: Options are included only if corresponding Requests are received.

Case 1: (OPTION_SIP_SERVER_D (21)) or both (OPTION_SIP_SERVER_D (21) and OPTION_SIP_SERVER_A (22)) and OPTION_DOMAIN_LIST(24) or OPTION_DNS_SERVERS (23) received in step 5

Options	Value/Remarks
option-code	OPTION_SIP_SERVER_D (21)
- option-len	Length of encoded domain address RFC 3319[51]
Domain-address 1	SS P-CSCF server domain Address RFC 3319[51]
option-code	OPTION_DNS_SERVERS (23)
- option-len	Length of encoded DNS server address RFC 3646[48]
Domain-address 1	SS DNS server IPv6 address RFC 3646[48]
option-code	OPTION_DOMAIN_LIST (24)
- option-len	Length of Domain search list
searchlist	List of Domain Names encoded as per RFC 1035 [52]

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Case 2: OPTION_SIP_SERVER_A (22) received in step 5

Options	Value/Remarks
option-code	OPTION_SIP_SERVER_A (22)
- option-len	128
Domain-address 1	IPv6 address of SS P-CSCF Server
option-code	OPTION_DNS_SERVERS (23)
- option-len	Length of encoded DNS server address RFC 3646[48]
Domain-address 1	SS DNS server IPv6 address RFC 3646[48]
option-code	OPTION_DOMAIN_LIST (24)
- option-len	Length of Domain search list
searchlist	List of Domain Names encoded as per RFC 1035 [52]

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

Step 7: DNS NAPTR Query

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	P-CSCF domain name received
QCLASS=	IN
QTYPE=	NAPTR

Step 8: DNS NAPTR Response

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in NAPTR Query
QCLASS=	IN
QTYPE=	NAPTR
NAPTR Records	NAPTR Records included for each Transport protocol (TLS, TCP, UDP) supported RFC 3263[50]

Step 9: DNS SRV Query

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Corresponding to the transport protocol selected by UE among those provided in DNS NAPTR Response
QCLASS=	IN
QTYPE=	SRV

Step 10: DNS SRV Response

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in SRV Query
QCLASS=	IN
QTYPE=	SRV
SRV Records	SRV Resource Record included providing the SS target server FQDN RFC 3263[50].

Step 11: DNS AAAA Query

Case 1: steps 7 to 10 executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among provided in step 10 based on priority and weight RFC 2728[56]
QCLASS=	IN
QTYPE=	AAAA

Case 2: steps 7 to 10 not executed:

Field	Value/Remarks
OPCODE=	SQUERY
QNAME=	Selected P-CSCF name among addresses provided in step 4 or 6.
QCLASS=	IN
QTYPE=	AAAA

Step 12: DNS AAAA Response

Field	Value/Remarks
OPCODE=	SQUERY, RESPONSE, AA
QNAME=	Same as received in AAAA Query
QCLASS=	IN
QTYPE=	AAAA
AAAA records	Includes resolved IP address(es).

7.6.5 Test requirements

1. In step 1, the UE shall send a PDP Context Request message.
2. After step 2, the UE shall either ignore the received address, or use the address received.
3. If the UE ignores the P-CSCF address in step 2, then the UE will send a DHCP query in step 3.
4. After steps 4 and 6, if a P-CSCF IPv6 address is received then the UE will consider the P-CSCF discovery procedure successful, else the UE will initiate a DNS query for domain address to IPv6 address translation.
5. In step 13, the UE shall send an initial REGISTER message using the discovered P-CSCF address.

7.7 Void

7.8 Void

7.9 P-CSCF Discovery from ISIM

7.9.1 Definition

Test to verify that the UE can acquire P-CSCF address(es) in home network from ISIM while UE is roaming. The test case is applicable for IMS security or GIBA.

7.9.2 Conformance requirement

[TS 24.229 clause B.2.2.1]:

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a GPRS attach procedure as specified in 3GPP TS 24.008 [8];

b) ensure that a PDP context used for SIP signalling according to the APN and GGSN selection criteria described in 3GPP TS 23.060 [4] and 3GPP TS 27.060 [10A] is available. This PDP context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the PDP context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

...

c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

I. ...

II. ...

III. The UE selects a P-CSCF from the list (see 3GPP TS 31.103 [15B]) stored in the ISIM.

IV. ...

...

The UE shall use method III to select the P-CSCF, if:

- a P-CSCF is to be discovered in the home network;
- the UE is roaming;
- either the UE does not contain the IMS management object, or the UE contains the IMS management object, but the IMS management object does not contain the P-CSCF list; and
- the ISIM residing in the UICC supports the P-CSCF list.

[TS 24.229 clause L.2.2.1]:

Prior to communication with the IM CN subsystem, the UE shall:

a) perform a EPS attach procedure as specified in 3GPP TS 24.301 [8J];

b) ensure that a EPS bearer context used for SIP signalling according to the APN and P-GW selection criteria described in 3GPP TS 23.401 [7B], is available. This EPS bearer context shall remain active throughout the period the UE is connected to the IM CN subsystem, i.e. from the initial registration and at least until the deregistration. As a result, the EPS bearer context provides the UE with information that makes the UE able to construct an IPv4 or an IPv6 address;

...

c) acquire a P-CSCF address(es).

The methods for P-CSCF discovery are:

I. ...

II. ...

III. The UE selects a P-CSCF from the list (see 3GPP TS 31.103 [15B]) stored in the ISIM.

IV. ...

...

The UE shall use method III to select the P-CSCF, if:

- a P-CSCF is to be discovered in the home network;
- the UE is roaming;
- either the UE does not contain the IMS management object, or the UE contains the IMS management object but the IMS management object does not contain the P-CSCF list; and
- the ISIM residing in the UICC supports the P-CSCF list.

Reference(s)

3GPP TS 24.229[10], clauses B.2.2.1 and L.2.2.1.

7.9.3 Test purpose

To verify that the UE is able to discover the P-CSCF address from ISIM if the UE is roaming and the UE is configured to discover the P-CSCF from the home network.

7.9.4 Method of test

Initial conditions

Cells activated on SS belong to a VPLMN SS is configured with the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE is equipped with a UICC that contains ISIM application. ISIM contains the address of P-CSCF within home network. UE has either EPS bearer context or GPRS PDP context activated .Within the context activation messaging from the SS the UE is supplied with a P-CSCF address different from the one that is found in the ISIM.

Related ICS/IXIT Statement(s)

P-CSCF is to be discovered in the home network (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Test procedure

1) IMS registration is initiated on the UE. Consequently the UE discovers the P-CSCF address from ISIM and sends an initial SIP REGISTER request to the discovered P-CSCF.

2) Continue test execution with the Generic test procedure, Annex C.2 or C.2a (GIBA), step 5.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE sends initial registration for IMS services to the P-CSCF discovered from ISIM
2			Continue with Annex C.2 or C.2a step 5	Execute the Generic test procedure Annex C.2 or step 5-11 or C.2a (GIBA only) step 5-9 in order to get the UE in a stable registered state

NOTE: The default messages contents in annex A are used with condition 'IMS security ' or 'GIBA' when applicable

7.9.5 Test requirements

1) In step 1, the UE shall send an initial REGISTER message to the P-CSCF address which has been configured to the ISIM.

8 Registration

TCP (***Transmission Control Protocol***) is applied as DL transport protocol to the present clause.

8.1 Initial registration

8.1.1 Definition and applicability

Test to verify that the UE can correctly register to IMS services when equipped with UICC that contains either both ISIM and USIM applications or only USIM application but not ISIM. The process consists of sending initial registration

to S-CSCF via the P-CSCF discovered, authenticating the user and finally subscribing the registration event package for the registered default public user identity. The test case is applicable for IMS security.

8.1.2 Conformance requirement

[TS 24.229, clause C.2]:

In case the UE is loaded with a UICC that contains a USIM but does not contain an ISIM, the UE shall:

- generate a private user identity;
- generate a temporary public user identity; and
- generate a home network domain name to address the SIP REGISTER request to.

All these three parameters are derived from the IMSI parameter in the USIM, according to the procedures described in 3GPP TS 23.003. Also in this case, the UE shall derive new values every time the UICC is changed, and shall discard existing values if the UICC is removed.

NOTE: If there is an ISIM and a USIM on a UICC, the ISIM is used for authentication to the IM CN subsystem, as described in 3GPP TS 33.203. See also subclause 5.1.1.1A.

[TS 24.229, clause 5.1.1.1A]:

The ISIM shall always be used for authentication to the IM CN subsystem, if it is present, as described in 3GPP TS 33.203.

The ISIM is preconfigured with all the necessary parameters to initiate the registration to the IM CN subsystem. These parameters include:

- the private user identity;
- one or more public user identities; and
- the home network domain name used to address the SIP REGISTER request

The first public user identity in the list stored in the ISIM is used in emergency registration requests.

In case the UE does not contain an ISIM, the UE shall:

- generate a private user identity;
- generate a temporary public user identity; and
- generate a home network domain name to address the SIP REGISTER request to;

in accordance with the procedures in clause C.2.

The temporary public user identity is only used in REGISTER requests, i.e. initial registration, re-registration, mobile-initiated deregistration.

The UE shall not reveal to the user the temporary public user identity if the temporary public user identity is barred. The temporary public user identity is not barred if received by the UE in the P-Associated-URI header.

If the UE is unable to derive the parameters in this subclause for any reason, then the UE shall not proceed with the request associated with the use of these parameters and will not be able to register to the IM CN subsystem.

[TS 24.229, clause 5.1.1.2.1]:

The initial registration procedure consists of the UE sending an unprotected REGISTER request and, if challenged depending on the security mechanism supported for this UE, sending the integrity-protected REGISTER request or other appropriate response to the challenge. The UE can register a public user identity with any of its contact addresses at any time after it has acquired an IP address, discovered a P-CSCF, and established an IP-CAN bearer that can be used for SIP signalling. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

When registering any public user identity belonging to the UE, the UE shall either use an already active pair of security associations or a TLS session to protect the REGISTER requests, or register the public user identity via a new initial registration procedure.

When binding any one of its public user identities to an additional contact address via a new initial registration procedure, the UE shall follow the procedures described in RFC 5626. The set of security associations or a TLS session resulting from this initial registration procedure will have no impact on the existing set of security associations or TLS sessions that have been established as a result of previous initial registration procedures. However, if the UE registers any one of its public user identities with a new contact address via a new initial registration procedure and does not employ the procedures described in RFC 5626, then the new set of security associations or TLS session shall replace any existing set of security association or TLS session.

If the UE detects that the existing security associations or TLS sessions associated with a given contact address are no longer active (e.g., after receiving no response to several protected messages), the UE shall:

- consider all previously registered public user identities bound to this security associations or TLS session that are only associated with this contact address as deregistered; and

- stop processing all associated ongoing dialogs and transactions that were using the security associations or TLS session associated with this contact address, if any (i.e. no further SIP signalling will be sent by the UE on behalf of these transactions or dialogs).

The UE shall send the unprotected REGISTER requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, or if the UE was pre-configured with the P-CSCF's IP address or domain name and was unable to obtain specific port information, the UE shall send the unprotected REGISTER request to the SIP default port values as specified in RFC 3261.

NOTE 1: The UE will only send further registration and subsequent SIP messages towards the same port of the P-CSCF for security mechanisms that do not require using negotiated ports for exchanging protected messages.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B. A public user identity may be input by the end user.

On sending an unprotected REGISTER request, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) containing the IP address or FQDN of the UE in the hostport parameter. If the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations, the UE shall include a "+sip.instance" header field parameter containing the instance ID. If the UE supports multiple registrations it shall include "reg-id" header field parameter as described in RFC 5626. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840;

d) a Via header field set to include the sent-by field containing the IP address or FQDN of the UE and the port number where the UE expects to receive the response to this request when UDPis used. For TCP, the response is received on the TCP connection on which the request was sent. For the UDP, the UE shall also include a "rport" header field parameter with no value in the Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with the registration, as described in draft-ietf-sipcore-keep;

NOTE 2: When sending the unprotected REGISTER request using UDP, the UE transmit the request from the same IP address and port on which it expects to receive the response to this request.

e) a registration expiration interval value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and

1) if GRUU is supported, the option-tag "gruu"; and

2) if multiple registrations is supported, the option-tag "outbound".

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter.

NOTE 4: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) store the expiration time of the registration for the public user identities found in the To header field value and bind it to the respective contact address of the UE;

b) store as the default public user identity the first URI on the list of URIs present in the P-Associated-URI header field and bind it to the respective contact address of the UE and the associated set of security associations or TLS session;

NOTE 5: When using the respective contact address and associated set of security associations or TLS session, the UE can utilize additional URIs contained in the P-Associated-URI header field and bound it to the respective contact address of the UE and the associated set of security associations or TLS session, e.g. for application purposes.

c) treat the identity under registration as a barred public user identity, if it is not included in the P-Associated-URI header field;

d) store the list of service route values contained in the Service-Route header field and bind the list to the contact address and the associated set of security associations or TLS session over which the REGISTER request was sent, in order to build a proper preloaded Route header field value for new dialogs and standalone transactions when using this contact address and the associated set of security associations or TLS session;

e) find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, and the UE supports GRUU (see table A.4, item A.4/53), then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered;

f) if the REGISTER request contained the "reg-id" and "+sip.instance" Contact header field parameter and the "outbound" option tag in a Supported header field, the UE shall check whether the option-tag "outbound" is present in the Require header field:

- if no option-tag "outbound" is present, the UE shall conclude that the S-CSCF does not support the registration procedure as described in RFC 5626, and the S-CSCF has followed the registration procedure as described in RFC 5627 or RFC 3261, i.e., if there is a previously registered contact address, the S-CSCF replaced the old contact address and associated information with the new contact address and associated information (see bullet e) above). Upon detecting that the S-CSCF does not support the registration procedure as defined in RFC 5626, the UE shall refrain from registering any additional IMS flows for the same private identity as described in RFC 5626; or

NOTE 6: Upon replaces the old contact address with the new contact address, the S-CSCF performs the network initiated deregistration procedure for the previously registered public user identities and the associated old contact address as described in subclause 5.4.1.5. Hence, the UE will receive a NOTIFY request informing the UE about the deregistration of the old contact address.

- if an option-tag "outbound" is present, the UE may establish additional IMS flows for the same private identity, as defined in RFC 5626;

g) store the announcement of media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field according to the procedures described in draft-dawes-dispatch-mediasec-parameter, if any; and

NOTE 7: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

h) if the Via header field contains a "keep" header field parameter with a value, unless the UE detects that it is not behind a NAT, start to send keep-alives associated with the registration towards the P-CSCF, as described in draft-ietf-sipcore-keep.

[TS 24.229, clause 5.1.1.2.2]:

On sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field, with:

- the "username" header field parameter, set to the value of the private user identity;

- the "realm" header field parameter, set to the domain name of the home network;

- the "uri" header field parameter, set to the SIP URI of the domain name of the home network;

- the "nonce" header field parameter, set to an empty value; and

- the "response" header field parameter, set to an empty value;

NOTE 1: If the UE specifies its FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security association. For details on the selection of the port values see 3GPP TS 33.203.

b) additionally for the Contact header field, if the REGISTER request is protected by a security association, include the protected server port value in the hostport parameter;

c) additionally for the Via header field, for UDP, if the REGISTER request is protected by a security association, include the protected server port value in the sent-by field; and

d) a Security-Client header field set to specify the signalling plane security mechanism the UE supports, the IPsec layer algorithms the UE supports and the parameters needed for the security association setup. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203. The syntax of the parameters needed for the security association setup is specified in annex H of 3GPP TS 33.203. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329. The UE shall support the IPsec layer algorithms for integrity and confidentiality protection as defined in 3GPP TS 33.203, and shall announce support for them according to the procedures defined in RFC 3329.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.2.1, the UE shall additionally:

1) If the UE supports multiple registrations and the REGISTER request contained the "+sip.instance" header field parameter and the "reg-id" header field parameter in the Contact header field, and the "outbound" option-tag in the Supported header field, the UE shall check whether the option-tag "outbound" is present in the Require header field. If the option-tag "outbound" is present, then the UE shall use the bidirectional flow as defined in RFC 5626 as follows:

a) for UDP, the bidirectional flow consists of two unidirectional flows, i.e. the first unidirectional flow is identified with the UE's protected client port, the P-CSCF's protected server port, and the respective IP addresses. The UE uses this flow to send the requests and responses to the P-CSCF. The second unidirectional flow is identified with the P-CSCF's protected client port, the UE's protected server port and the IP addresses. The second unidirectional flow is used by the UE to receive the requests and responses from the P-CSCF; or

b) for TCP, the bidirectional flow is the TCP connection between the UE and the P-CSCF. This TCP connection was established by the UE, i.e. from the UE's protected client port and the UE's IP address to the P-CSCF's protected server port and the P-CSCF's IP address. This TCP connection is used to exchange SIP messages between the UE and the P-CSCF; and

2) set the security association lifetime to the longest of either the previously existing security association lifetime (if available), or the lifetime of the just completed registration plus 30 seconds.

NOTE 3: If the UE receives Authentication-Info, it will proceed as described in RFC 3310.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

[TS 24.229, clause 5.1.1.5.1]:

Authentication is performed during initial registration. A UE can be re-authenticated during subsequent reregistrations, deregistrations or registrations of additional public user identities. When the network requires authentication or re-authentication of the UE, the UE will receive a 401 (Unauthorized) response to the REGISTER request.

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

1) extract the RAND and AUTN parameters;

2) check the validity of a received authentication challenge, as described in 3GPP TS 33.203 i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

3) check the existence of the Security-Server header field as described in RFC 3329. If the Security-Server header field is not present or it does not contain the parameters required for the setup of the set of security associations (see annex H of 3GPP TS 33.203), the UE shall abandon the authentication procedure and send a new REGISTER request with a new Call-ID.

In the case that the 401 (Unauthorized) response to the REGISTER request is deemed to be valid the UE shall:

1) calculate the RES parameter and derive the keys CK and IK from RAND as described in 3GPP TS 33.203;

2) set up a temporary set of security associations for this registration based on the static list and parameters the UE received in the 401 (Unauthorized) response and its capabilities sent in the Security-Client header field in the REGISTER request. The UE sets up the temporary set of security associations using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE and using IK and CK (only if encryption enabled) as the shared key. The UE shall use the parameters received in the Security-Server header field to setup the temporary set of security associations. The UE shall set a temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer;

3) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter.

NOTE 1: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

4) send another REGISTER request towards the protected server port indicated in the response using the temporary set of security associations to protect the message. The header fields are populated as defined for the initial REGISTER request that was challenged with the received 401 (Unauthorized) response, with the addition that the UE shall include an Authorization header field containing:

- the "realm" header field parameter set to the value as received in the "realm" WWW-Authenticate header field parameter;

- the "username" header field parameter, set to the value of the private user identity;
- the "response" header field parameter that contains the RES parameter, as described in RFC 3310;
- the "uri" header field parameter, set to the SIP URI of the domain name of the home network;
- the "algorithm" header field parameter, set to the value received in the 401 (Unauthorized) response; and
- the "nonce" header field parameter, set to the value received in the 401 (Unauthorized) response.

The UE shall also insert the Security-Client header field that is identical to the Security-Client header field that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header field into the request, by mirroring in it the content of the Security-Server header field received in the 401 (Unauthorized) response. The UE shall set the Call-ID of the security association protected REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

On receiving the 200 (OK) response for the security association protected REGISTER request registering a public user identity with the associated contact address, the UE shall:

- change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and
- if this is the only set of security associations available toward the P-CSCF, use the newly established set of security associations for further messages sent towards the P-CSCF. If there are additional sets of security associations (e.g. due to registration of multiple contact addresses), the UE can either use them or use the newly established set of security associations for further messages sent towards the P-CSCF as appropriate.

NOTE 2: If the UE has registered multiple contact addresses, the UE can either send requests towards the P-CSCF over the newly established set of security associations, or use different UE's contact address and associated set of security associations when sending the requests towards the P-CSCF. Responses towards the P-CSCF that are sent via UDP will be sent over the same set of security associations that the related request was received on. Responses towards the P-CSCF that are sent via TCP will be sent over the same set of security associations that the related request was received on.

When the first request or response protected with the newly established set of security associations is received from the P-CSCF or when the lifetime of the old set of security associations expires, the UE shall delete the old set of security associations and related keys it may have with the P-CSCF after all SIP transactions that use the old set of security associations are completed.

[TS 24.229, clause 5.1.1.3]:

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the reg event package for the public user identity registered at the user's registrar (S-CSCF) as described in RFC 3680.

The UE shall subscribe to the reg event package upon registering a new contact address via an initial registration procedure. If the UE receives a NOTIFY request via the newly established subscription dialog and via the previously established subscription dialogs (there will be at least one), the UE may terminate the previously established subscription dialogs and keep only the newly established subscription dialog.

The UE shall use the default public user identity for subscription to the registration-state event package, if the public user identity that was used for initial registration is a barred public user identity. The UE may use either the default public user identity or the public user identity used for initial registration for the subscription to the registration-state event package, if the initial public user identity that was used for initial registration is not barred.

On sending a SUBSCRIBE request, the UE shall populate the header fields as follows:

a) a Request-URI set to the resource to which the UE wants to be subscribed to, i.e. to a SIP URI that contains the public user identity used for subscription;

b) a From header field set to a SIP URI that contains the public user identity used for subscription;

c) a To header field set to a SIP URI that contains the public user identity used for subscription;

d) an Event header field set to the "reg" event package;

e) an Expires header field set to 600 000 seconds as the value desired for the duration of the subscription;

f) void; and

g) void.

Upon receipt of a 2xx response to the SUBSCRIBE request, the UE shall store the information for the established dialog and the expiration time as indicated in the Expires header field of the received response.

[TS 24.229, clause 5.1.2.1]:

Upon receipt of a 2xx response to the SUBSCRIBE request the UE shall maintain the generated dialog (identified by the values of the Call-ID header field, and the values of tags in To and From header fields).

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package the UE shall perform the following actions:

- if a state attribute "active", i.e. registered is received for one or more public user identities, the UE shall store the indicated public user identities as registered;

- if a state attribute "active" is received, and the UE supports GRUU (see table A.4, item A.4/53), then for each public user identity indicated in the notification that contains a <pub-gruu> element or a <temp-gruu> element or both (as defined in RFC 5628) then the UE shall store the value of those elements in association with the public user identity;

- if a state attribute "terminated", i.e. deregistered is received for one or more public user identities, the UE shall store the indicated public user identities as deregistered and shall remove any associated GRUUs.

NOTE 1: There may be public user identities which are automatically registered within the registrar (S-CSCF) of the user upon registration of one public user identity or when S-CSCF receives a Push-Profile-Request (PPR) from the HSS (as described in 3GPP TS 29.228) changing the status of a public user identity associated with a registered implicit set from barred to non-barred. Usually these automatically or implicitly registered public user identities belong to the same service profile of the user and they might not be available within the UE. The implicitly registered public user identities may also belong to different service profiles. The here-described procedures provide a different mechanism (to the 200 (OK) response to the REGISTER request) to inform the UE about these automatically registered public user identities.

NOTE 2: RFC 5628 provides guidance on the management of temporary GRUUs, utilizing information provided in the reg event notification.

[TS 24.229, clause 5.1.2A.1.1]:

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

When the UE sends any request using a given contact address, the UE shall:

- if IMS AKA is in use as a security mechanism:

  a) if the UE has not obtained a GRUU, populate the Contact header field of the request with the protected server port and the respective contact address; and

  b) include the protected server port and the respective contact address in the Via header field entry relating to the UE;

- if SIP digest without TLS is in use as a security mechanism:

  a) if the UE has not obtained a GRUU, populate the Contact header field of the request with the port value of an unprotected port and the contact address where the UE expects to receive subsequent mid-dialog requests; and

  b) populate the Via header field of the request with the port value of an unprotected port and the respective contact address where the UE expects to receive responses to the request;

...

If available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall insert a P-Access-Network-Info header field into any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method (see subclause 7.2A.4).

NOTE 13: During the dialog, the points of attachment to the IP-CAN of the UE may change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header field in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header field value for all new dialogs and standalone transactions. The UE shall build a list of Route header field values made out of the following, in this order:

a) the P-CSCF URI containing the IP address or the FQDN learnt through the P-CSCF discovery procedures; and

b) the P-CSCF port based on the security mechanism in use:

- if IMS AKA or SIP digest with TLS is in use as a security mechanism, the protected server port learnt during the registration procedure;

- if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled authentication is in use as a security mechanism, the unprotected server port used during the registration procedure;

c) and the values received in the Service-Route header field saved from the 200 (OK) response to the last registration or re-registration of the public user identity with associated contact address.

[TS 24.341, clause 5.3.2.2]

On sending a REGISTER request, the SM-over-IP receiver shall indicate its capability to receive traditional short messages over IMS network by including a "+g.3gpp.smsip" parameter into the Contact header according to RFC 3840.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.1.1A, 5.1.1.2.1 5.1.1.2, 5.1.1.35.1.1.5.1, 5.1.2.1, 5.1.2A.1, C.2 and TS 24.341, clause 5.3.2.2.

8.1.3 Test purpose

1) To verify that UE correctly derives a private user identity, a temporary public user identity and a home network domain name from the IMSI parameter in the USIM if no ISIM is available on the UICC, according to the procedures described in 3GPP TS 23.003 [32] clause 13 or alternatively uses the values retrieved from ISIM, if ISIM is present; and

2) To verify that the UE sends a correctly composed initial REGISTER request to S-CSCF via the discovered P-CSCF, according to 3GPP TS 24.229 [10] clause 5.1.1.2; and TS 24.341 [90] clause 5.3.2.2 (if UE supports SM-over-IP receiver marked as yes)

3) To verify that after receiving a valid 401 (Unauthorized) response from S-CSCF for the initial REGISTER sent, the UE correctly authenticates itself by sending another REGISTER request with correctly composed Authorization header using AKAv1-MD5 algorithm (as described in RFC 3310 [17]); and

4) To verify that the UE announces to support the "ipsec-3gpp" security mechanism together the IPsec layer algorithms for integrity (Rel-5 onwards) and confidentiality (Rel-6 onwards) protection (as defined in 3GPP TS 33.203)according to the procedures defined in RFC 3329 [21]; and

5) To verify that the UE supports the IPsec layer algorithms for integrity (Rel-5 onwards) and confidentiality (Rel-6 onwards) protection as defined in 3GPP TS 33.203and uses the one that is preferred by the P-CSCF according to the procedures defined in RFC 3329 [21]; and

6) To verify that the UE sets up two pairs of security associations as defined in 3GPP TS 33.203 [14] clause 7 and uses those for sending the REGISTER request to authenticate itself and for sending any other subsequent request; and

7) To verify that after receiving a valid 200 OK response from S-CSCF for the REGISTER sent for authentication, the UE stores the default public user identity and information about barred user identities; and

8) To verify that after receiving a valid 200 OK response from S-CSCF for the REGISTER sent for authentication, the UE subscribes to the reg event package for the public user identity registered at the users registrar (S-CSCF) as described in RFC 3680 [22]; and

9) To verify that the UE uses the default public user identity for subscription to the registration-state event package, when the public user identity that was used for initial registration is a barred public user identity; and

10) To verify that the UE uses the stored service route for routing the SUBSCRIBE sent; and

11) To verify that after receiving a valid 200 OK response from S-CSCF to the SUBSCRIBE sent for registration event package, the UE maintains the generated dialog; and

12) To verify that after receiving a valid NOTIFY for the registration event package, the UE will update and store the registration state of the indicated public user identities accordingly (as specified in RFC 3680 [22] clause 5); and

13) To verify that the UE responds the received valid NOTIFY with 200 OK.

8.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services, but has performed the generic test procedure in Annex C.2 up to step 3.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Related ICS/IXIT Statement(s)

- UE supports IPSec ESP confidentiality protection (Yes/No)
- IMS security (Yes/No)
- obtaining and using GRUUs in the Session Initiation Protocol (SIP) (Yes/No)
- UE supports MTSI (Yes/No)
- UE supports SM-over-IP receiver (Yes/No)

Test procedure

1) IMS registration is initiated on the UE. SS waits for the UE to send an initial REGISTER request.

2) SS responds to the initial REGISTER request with a valid 401 Unauthorized response, headers populated according to the 401 response common message definition.

3) SS waits for the UE to set up a temporary set of security associations and send another REGISTER request, over those security associations.

4) SS responds to the second REGISTER request with valid 200 OK response, sent over the same temporary set of security associations that the UE used for sending the REGISTER request. SS shall populate the headers of the 200 OK response according to the 200 response for REGISTER common message definition.

5) SS waits for the UE to send a SUBSCRIBE request over the newly established security associations.

6) SS responds to the SUBSCRIBE request with a valid 200 OK response, headers populated according to the 200 response for SUBSCRIBE common message definition.

7) SS sends UE a NOTIFY request for the subscribed registration event package. In the request the Request URI, headers and the request body shall be populated according to the NOTIFY common message definition.

8) SS waits for the UE to respond the NOTIFY with 200 OK response.

NOTE: This test case shall be run twice in order to test that the UE correctly supports both HMAC-MD5-96 and HMAC-SHA-1-96 algorithms. For each test round the name of the corresponding algorithm shall be configured into px_IpSecAlgorithm PIXIT.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE sends initial registration for IMS services.
2	←		401 Unauthorized	The SS responds with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network.
3	→		REGISTER	UE completes the security negotiation procedures, sets up a temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials.
4	←		200 OK	The SS responds with 200 OK.
5	→		SUBSCRIBE	UE subscribes to its registration event package.
6	←		200 OK	The SS responds SUBSCRIBE with 200 OK
7	←		NOTIFY	The SS sends initial NOTIFY for registration event package, containing full registration state information for the registered public user identity in the XML body
8	→		200 OK	The UE responds the NOTIFY with 200 OK

Specific Message Contents

REGISTER (Step 1)

Use the default message 'REGISTER' in annex A.1.1 with condition A1 "Initial unprotected REGISTER" and condition A6 'The UE supports SM-over-IP receiver' (if UE supports SM-over-IP receiver marked as yes)

401 Unauthorized for REGISTER (Step 2)

Use the default message '401 Unauthorized for REGISTER' in annex A.1.2

REGISTER (Step 3)

Use the default message 'REGISTER' in annex A.1.1 with condition A2 "Subsequent REGISTER sent over security associations" and condition A6 'The UE supports SM-over-IP receiver' (if UE supports SM-over-IP receiver SM marked as yes)

200 OK for REGISTER (Step 4)

Use the default message '200 OK for REGISTER' in annex A.1.3

SUBSCRIBE (Step 5)

Use the default message 'SUBSCRIBE for reg-event package' in annex A.1.4

200 OK for SUBSCRIBE (Step 6)

Use the default message '200 OK for SUBSCRIBE' in annex A.1.5

NOTIFY (Step 7)

Use the default message 'NOTIFY for reg-event package' in annex A.1.6

200 OK for NOTIFY (Step 8)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

8.1.5 Test requirements

If the UICC card equipped to the UE contains ISIM, the UE must read the following parameters from ISIM (instead of deriving them from USIM) and use they for the REGISTER requests:

- the private user identity; and
- the temporary public user identity; and
- the home network domain name.

Step 3: SS shall check that in accordance to the 3GPP TS 24.229 [10] clause 5.1.1.5 the UE sends another REGISTER request as follows:

a) the UE sets up the temporary set of security associations between the ports announced in Security-Client header (UE) in the REGISTER request and Security-Server header (SS) in the 401 Unauthorized response; and

b) the UE uses the most preferred mechanism and algorithm returned by the SS and supported by the UE for the temporary set of security associations; and

c) the UE uses IK derived from RAND as the shared key for integrity and confidentiality protection (if the UE supports IPSec ESP confidentiality protection) for the temporary set of security associations; and

d) the UE sends the second REGISTER over the temporary set of security associations; and

Step 5: SS shall check that, in accordance to the 3GPP TS 24.229 [10] clause 5.1.1.3, the UE sends a SUBSCRIBE request for registration event package over the newly established set of security associations.

NOTE: If the UE specifies its FQDN in the host parameter in the Contact header and in the sent-by field in the Via header (within any of the request sent by the UE), then SS has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association (or to the unprotected port in the initial REGISTER).

8.2 User Initiated Re-Registration

8.2.1 Definition

Test to verify that the UE can re-register a previously registered public user identity at any time. This process is described in 3GPP TS 24.229 [10], clause 5.1.1.4. The test case is applicable for IMS security.

8.2.2 Conformance requirement

[TS 24.229, clause 5.1.1.4.1]:

The UE can perform the reregistration of a previously registered public user identity bound to any one of its contact addresses and the associated set of security associations or TLS sessions at any time after the initial registration has been completed.

The UE can perform the reregistration of a previously registered public user identity over any existing set of security associations or TLS session that is associated with the related contact address.

The UE can perform the reregistration of a previously registered public user identity via an initial registration as specified in subclause 5.1.1.2, when binding the previously registered public user identity to new contact address.

The UE can perform registration of additional public user identities at any time after the initial registration has been completed. The UE shall perform the registration of additional public user identities either:

- over the existing set of security associations or TLS sessions, if appropriate to the security mechanism in use, that is associated with the related contact address; or

- via an initial registration as specified in subclause 5.1.1.2.

The UE can fetch bindings as defined in RFC 3261 at any time after the initial registration has been completed. The procedure for fetching bindings is the same as for a reregistration except that the REGISTER request does not contain a Contact header field.

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister an already registered public user identity either 600 seconds before the expiration time if the previous registration was for greater than 1200 seconds, or when half of the time has expired if the previous registration was for 1200 seconds or less, or when the UE intends to update its capabilities according to RFC 3840 or when the UE needs to modify the ICSI values that the UE intends to use in a g.3gpp.icsi-ref media feature tag or IARI values that the UE intends to use in the g.3gpp.iari-ref media feature tag.

When sending a protected REGISTER request, the UE shall use a security association or TLS session associated with the contact address used to send the request, see 3GPP TS 33.203, established as a result of an earlier initial registration.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) that contain(s) in the hostport parameter the IP address or FQDN of the UE, and containing the instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations. If the UE support multiple registrations, it shall include "reg-id" header field as described in RFC 5626. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 for the IMS communication it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840;

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field. For the TCP, the response is received on the TCP connection on which the request was sent. If the UE previously has previously negotiated sending of keep-alives associated with the registration, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate continuous support to send keep-alives, as described in draft-ietf-sipcore-keep;

e) a registration expiration interval value, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 1: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and if GRUU is supported, the option-tag "gruu";

h) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter.

NOTE 2: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) bind the new expiration time of the registration for this public user identity found in the To header field value to the contact address used in this registration;

b) store the list of service route values contained in the Service-Route header field and bind the list to the contact address used in registration, in order to build a proper preloaded Route header field value for new dialogs and standalone transactions when using the respective contact address;

NOTE 3: If the list of Service-Route headers saved from a previous registration and bound to this contact address and the associated set of security associations or TLS session already exist, then the received list of Service-Route headers replaces the old list.

NOTE 4: The UE can utilize additional URIs contained in the P-Associated-URI header field, e.g. for application purposes.

c) find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, and the UE supports GRUU (see table A.4, item A.4/53), then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered;

d) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter; and

NOTE 5: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

e) if the Via header field contains a "keep" header field parameter with a value, continue to send keep-alives as described in draft-ietf-sipcore-keep, towards the P-CSCF.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

[TS 24.229, clause 5.1.1.4.2]:

On sending a REGISTER request, as defined in subclause 5.1.1.4.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field, with:

- the "username" header field parameter set to the value of the private user identity;
- the "realm" header field parameter directive, set to the value as received in the "realm" WWW-Authenticate header field parameter;
- the "uri" header field parameter, set to the SIP URI of the domain name of the home network;
- the "nonce" header field parameter, set to last received nonce value; and
- the "response" header field parameter, set to the last calculated response value;

NOTE 1: If the UE specifies its FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203.

NOTE 3: If the UE is setting up an additional registration using procedures specified in RFC 5626 and the UE accesses the network through 3GPP or 3GPP2 systems without any NAT, the flow is considered to be "logical flow".

b) additionally for the Contact header field, include the protected server port value in the hostport parameter;

c) additionally for the Via header field, for UDP, if the REGISTER request is protected by a security association, include the protected server port value in the sent-by field;

d) a Security-Client header field, set to specify the signalling plane security mechanism it supports, the IPsec layer algorithms for security and confidentiality protection it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 and RFC 3329; and

e) a Security-Verify header field that contains the content of the Security-Server header field received in the 401 (Unauthorized) response of the last successful authentication.

On receiving the 200 (OK) response to the REGISTER request, the UE shall additionally:

a) set the security association lifetime associated with this contact address and the associated set of security associations to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds.

NOTE 4: If the UE receives Authentication-Info, it will proceed as described in RFC 3310.

Reference(s)

3GPP TS 24.229[10], clause s 5.1.1.4.1 and 5.1.1.4.2.

8.2.3 Test purpose

1) To verify that the UE can re-register a previously registered public user identity at either 600 seconds before the expiration time if the initial registration was for greater than 1200 seconds, or when half of the time has expired if the initial registration was for 1200 seconds or less; and

2) Extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration; and

3) To verify that the UE populates the header field in the REGISTER request with From, To, Via, Contact, Authorization, Expires, Security-Client, Security-verify, Supported, and P-Access-Network-Info headers; and

4) Upon receiving 200 OK for REGISTER, the UE shall store the new expiration time of the registration for this public user identity, the list of URIs contained in the P-Associated-URI header value and use these values in the next re-register request.

8.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services, but has an active PDP context and has discovered the SS as P-CSCF by executing the generic test procedure in Annex C.2 up to step 3.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

UE supports IPSec ESP confidentiality protection (Yes/No)

Test procedure

1-8) The same procedure as in subclause 8.1.4 are used with the exception that the SS sets the expiration time to 120 seconds in Step 4.

9) Before half of the time has expired from the initial registration SS receives re-register message request with the From, To, Via, Contact, Authorization, Expires, Security-Client, Security-verify, Supported, and P-Access-Network-Info header fields.

10) SS responds to the REGISTER request with valid 200 OK response with the list of URIs contained in the P-Associated-URI header value, the new expiration time (1200 seconds) of the registration for this public user identity.

11) SS waits for the REGISTER request and verifies it is received at least 600 seconds before the expected expiration time.

12) SS responds to the REGISTER request with valid 200 OK response with the list of URIs contained in the P-Associated-URI header value, the new expiration time (1800 seconds) of the registration for this public user identity.

13) SS waits for the REGISTER request and verifies it is received at least 600 seconds before the expected expiration time.

14) SS responds to the REGISTER request with valid 200 OK response. SS shall populate the headers of the 200 OK response according to the 200 response for REGISTER common message definition.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-8			Messages in Initial Registration Test case (subclause 8.1.4)	The same messages as in subclause 8.1.4 are used with the exception that in Step 4, the SS responds with 200 OK indicating 120 seconds expiration time.
9	→		REGISTER	The SS receives REGISTER from the UE 60 seconds before the expiration time set in the initial registration request.
10	←		200 OK	The SS responds with 200 OK indicating 1200 seconds expiration time.
11	→		REGISTER	The SS receives REGISTER from the UE 600 seconds before the expiration time set in step 10.
12	←		200 OK	The SS responds with 200 OK indicating 1800 seconds expiration time.
13	→		REGISTER	The SS receives REGISTER from the UE 600 seconds before the expiration time set in step 12
14	←		200 OK	The SS responds with 200 OK indicating the default expiration time.

Specific Message Contents

Messages in Step 1-8

Messages in Step 1-8 are the same as those specified in subclause 8.1.4 with the following exception for the 200 OK for REGISTER in Step 4:

Use the default message '200 OK for REGISTER' in annex A.1.3 with the following exceptions:

Header/param	Value/remark
Contact	
expires	120

REGISTER (Step 9)

Use the default message 'REGISTER' in annex A.1.1 with condition A2 "Subsequent REGISTER sent over security associations" and with the following exceptions:

Header/param	Value/remark
Security-Client	
spi-c	new SPI number of the inbound SA at the protected client port, shall be different than in step 3
spi-s	new SPI number of the inbound SA at the protected server port, shall be different than in step 3
port-c	new protected client port, shall be different than in step 3
port-s	Same value as in the previous REGISTER

200 OK for REGISTER (Step 10)

Use the default message '200 OK for REGISTER' in annex A.1.3 with the following exceptions:

Header/param	Value/remark
Contact	
expires	1200

REGISTER (Step 11)

Use the default message 'REGISTER' in annex A.1.1 with condition A2 "Subsequent REGISTER sent over security associations" and with the following exceptions:

Header/param	Value/remark
Security-Client	
spi-c	new SPI number of the inbound SA at the protected client port, shall be different than in step 3 but may or may not be the same as in step 9
spi-s	new SPI number of the inbound SA at the protected server port, shall be different than in step 3 but may or may not be the same as in step 9
port-c	new protected client port, shall be different than in step 3 but may or may not be the same as in step 9
port-s	Same value as in the previous REGISTER

200 OK for REGISTER (Step 12)

Use the default message '200 OK for REGISTER' in annex A.1.3 with the following exceptions:

Header/param	Value/remark
Contact	
expires	1800

REGISTER (Step 13)

Use the default message 'REGISTER' in annex A.1.1 with condition A2 "Subsequent REGISTER sent over security associations" and with the following exceptions:

Header/param	Value/remark
Security-Client	
spi-c	new SPI number of the inbound SA at the protected client port, shall be different than in step 3 but may or may not be the same as in step 9 or step 11
spi-s	new SPI number of the inbound SA at the protected server port, shall be different than in step 3 but may or may not be the same as in step 9 or step 11
port-c	new protected client, shall be different than in step 3 but may or may not be the same as in step 9 or step 11
port-s	Same value as in the previous REGISTER

200 OK for REGISTER (Step 14)

Use the default message '200 OK for REGISTER' in annex A.1.3.

8.2.5 Test requirements

1. The UE shall in step 9 send the REGISTER request within 60 seconds from the time instant that it receives 200 OK in step 4 from the SS.
2. The UE shall in step 11 send the REGISTER request within 600 seconds from the time instant that it receives 200 OK from the SS in step 10.
3. The UE shall in step 13 send the REGISTER request within 1200 seconds from the time instant that it receives 200 OK from the SS in step 12.

8.3 Mobile Initiated Deregistration

8.3.1 Definition and applicability

Test to verify that the UE can perform a correct de-registration procedure. This process is described in 3GPP TS 24.229 [10], clause 5.1.1.6. The test case is applicable for IMS security.

8.3.2 Conformance requirement

[TS 24.229, clause 5.1.1.6.1]:

The UE can deregister a public user identity that it has previously registered with its contact address at any time. The UE shall protect the REGISTER request using a security association or TLS session that is associated with contact address, see 3GPP TS 33.203, established as a result of an earlier registration, if one is available.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B.

Prior to sending a REGISTER request for deregistration, the UE shall release all dialogs that were using the contact addresses that is going to be deregistered and related to the public user identity that is going to be deregistered or to one of the implicitly registered public user identities. However:

- if the dialog that was established by the UE subscribing to the reg event package used the public user identity that is going to be deregistered; and
- this dialog is the only remaining dialog used for subscription to reg event package of the user, i.e. there are no other contact addresses registered with associated subscription to the reg event package of the user;

then the UE shall not release this dialog.

On sending a REGISTER request that will remove the binding between the public user identity and one of its contact addresses, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be deregistered;

b) a To header field set to the SIP URI that contains the public user identity to be deregistered;

c) a Contact header field set to the SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN, and containing the Instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations. If the UE supports multiple registrations, it shall include "reg-id" header field parameter as described in RFC 5626;

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field;

e) a registration expiration interval value set to the value of zero, appropriate to the deregistration requirements of the user;

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

h) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter.

NOTE 1: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

For a public user identity that the UE has registered with multiple contact addresses (e.g. via different P-CSCFs), the UE shall also be able to deregister multiple contact addresses, bound to its public user identity, via single deregistration procedure as specified in RFC 3261. The UE shall send a single REGISTER request, using one of its contact addresses and the associated set of security associations or TLS session, containing a list of Contact headers. Each Contact header in the list shall contain the contact addresses that the UE wants to deregister with the "expires" parameter containing the value equal zero.

The UE can deregister all contact addresses bound to its public user identity and associated with its private user identity. The UE shall send a single REGISTER request, using one of its contact addresses and the associated set of security associations or TLS session, containing a public user identity that is being deregistered in the To header field, and a single Contact header field with value of "*" and the Expires header field with a value of "0".

NOTE 2: All entities subscribed to the reg event package of the user will be inform via NOTIFY request which contact addresses bound to the public user identity have been deregistered.

When a 401 (Unauthorized) response to a REGISTER request is received the UE shall behave as described in subclause 5.1.1.5.1.

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

- remove all registration details relating to this public user identity and the associated contact address.

- store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter.

NOTE 9: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

If there are no more public user identities registered with this contact address, the UE shall delete any stored media plane security mechanisms and related keys and any security associations or TLS sessions and related keys it may have towards the IM CN subsystem.

If all public user identities are deregistered and all security association or TLS session is removed, then the UE shall consider subscription to the reg event package cancelled (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header field containing a value of zero).

[TS 24.229, clause 5.1.1.6.2]:

On sending a REGISTER request, as defined in subclause 5.1.1.6.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field, with:

- the "username" header field parameter, set to the value of the private user identity;

- the "realm" header field parameter, set to the value as received in the "realm" WWW-Authenticate header field parameter;

- the "uri" header field parameter, set to the SIP URI of the domain name of the home network;

- the "nonce" header field parameter, set to last received nonce value; and

- the response directive, set to the last calculated response value;

b) additionally for each Contact header field and associated contact address, include the associated protected server port value in the hostport parameter;

c) additionally for the Via header field, include the protected server port value bound to the security association in the sent-by field;

NOTE 1: If the UE specifies its FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

d) a Security-Client header field, set to specify the signalling plane security mechanisms it supports, the IPsec layer algorithms for integrity and confidentiality protection it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 and RFC 3329; and

e) a Security-Verify header field that contains the content of the Security-Server header field received in the 401 (Unauthorized) response of the last successful authentication.

NOTE 2: When the UE has received the 200 (OK) response for the REGISTER request of the only public user identity currently registered with this contact address and its associated set of implicitly registered public user identities (i.e. no other public user identity is registered), the UE removes the security association (between the P-CSCF and the UE) that were using this contact address. Therefore further SIP signalling using this security association (e.g. the NOTIFY request containing the deregistration event) will not reach the UE.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.1.6.1 and 5.1.1.6.2.

8.3.3 Test purpose

1) To verify that the UE sends a correctly composed initial REGISTER request with an expiration interval value set to 0 to S-CSCF via the discovered P-CSCF, according to 3GPP TS 24.229 [10] clause 5.1.1.6.

8.3.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is registered to IMS services by performing the generic registration test procedure in Annex C.2 up to the last step.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203[14] clause 6.1 and RFC 3310 [17].

Related ICS/IXIT Statement(s)

Method of triggering the UE to deregister from IMS services Yes/No

IMS security (Yes/No)

Test procedure

1) The UE is triggered by MMI to initiate a deregistration procedure

2) IMS deregistration is initiated on the UE. SS waits the UE to send a REGISTER request, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.6

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-2			Steps 1-2 defined in Annex C.30	

8.3.5 Test Requirements

SS shall check in step 1 that the de-register request sent by the UE have the headers correctly populated as per the default message 'REGISTER' in annex A.1.1condition A2, except for the headers described in 8.3.4.

8.4 Invalid behaviour- 423 Interval too brief

8.4.1 Definition and applicability

Test to verify that the UE sends another REGISTER request using a correct expiration timer when a registration attempt was rejected with a 423 (Interval Too Brief) response. The test case is applicable for IMS security.

8.4.2 Conformance requirement

On receiving a 423 (Interval Too Brief) response to the REGISTER request, the UE shall:

- send another REGISTER request populating the registration expiration interval value with an expiration timer of at least the value received in the Min-Expires header field of the 423 (Interval Too Brief) response.

Reference(s)

3GPP TS 24.229[10], clause 5.1.1.2.1.

8.4.3 Test purpose

To verify that after receiving a valid 423 (Interval Too Brief) response to the REGISTER request, the UE sends another REGISTER request populating the Expires header or the expires parameter in the Contact header with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

8.4.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services, but has an active PDP context and has discovered the SS as P-CSCF by executing the generic test procedure in Annex C.2 up to step 3.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols.

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

Test procedure

1 IMS registration is initiated on the UE. SS waits for the UE to send an initial REGISTER request.

2 SS responds to the initial REGISTER request with a 423 (Interval Too Brief) response.

3 SS waits for the UE to send another REGISTER request populating the Expires header or the expires parameter in the Contact header with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

4 Continue test execution with the Generic test procedure in Annex C.2, step 5, with the modifications listed below.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE sends initial registration for IMS services.
2	←		423 Interval Too Brief	The SS responds with a 423 (Interval Too Brief) too brief response to the REGISTER request with T value in Min-Expires header.
3	→		REGISTER	UE sends a new REGISTER request with expires parameter value set to Tmod (equal or greater to T value in Min-Expires header of 423 (Interval Too Brief)).
4	←→		Continue with Annex C.2 step 5	Execute the Generic test procedure Annex C.2 steps 5-11 in order to get the UE in a stable registered state.

Specific Message Contents

REGISTER (Step 1)

Use the default message 'REGISTER' in annex A.1.1 with condition A1 'Initial unprotected REGISTER'.

423 Interval Too Brief for REGISTER (Step 2)

Use the default message '423 Interval Too Brief for REGISTER' in annex A.1.7 with the following exception:

Header/param	Value/remark
Min-Expires	
delta-seconds	*800000* (referred to as T in the test procedure and test requirement)

REGISTER (Step 3)

Use the default message 'REGISTER' in annex A.1.1 with condition A1 'Initial unprotected REGISTER' with the following exceptions:

Header/param	Value/remark
Contact	
expires	*800000* (referred to as Tmod in the expected sequence) (if present, see Rule 1)
Expires	(if present, see Rule 1)
delta-seconds	*800000* (referred to as Tmod in the expected sequence)
CSeq	
value	must be incremented from the previous REGISTER

Rule 1: The REGISTER request must contain either an Expires header or an expires parameter in the Contact header. If both are present the value of Expires header is not important.

Modifications to steps detailed in Appendix C.2:

REGISTER (Step 6)

Header/param	Value/remark
Contact	
expires	*800000* (if present)
Expires	(if present)
delta-seconds	*800000*

200 OK (Step 7)

Header/param	Value/remark
Contact	
expires	800000

8.4.5 Test requirements

Step 3: The UE shall send another REGISTER request populating the Expires header or the expires parameter in the Contact header with an expiration timer of at least the value received in the Min-Expires header of the 423 (Interval Too Brief) response.

8.5 Void

8.6 Void

8.7 Void

8.8 Void

8.9 Void

8.10 Initial registration using GIBA

8.10.1 Definition and applicability

Test to verify that the UE can correctly register to IMS services when equipped with UICC that contains ISIM and USIM applications or only USIM application. The process consists of sending initial registration to S-CSCF via the P-CSCF discovered and subscribing the registration event package for the registered default public user identity. The test case is applicable for UE supporting GIBA only.

8.10.2 Conformance requirement

[TS 24.229, clause 5.1.1.2.1]

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B. A public user identity may be input by the end user.

On sending an unprotected REGISTER request, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) containing the IP address or FQDN of the UE in the hostport parameter. If the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations, the UE shall include a "+sip.instance" header field parameter containing the instance ID. If the UE supports multiple registrations it shall include "reg-id" header field parameter as described in RFC 5626. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840;

d) a Via header field set to include the sent-by field containing the IP address or FQDN of the UE and the port number where the UE expects to receive the response to this request when UDPis used. For TCP, the response is received on the TCP connection on which the request was sent. For the UDP, the UE shall also include a "rport" header field parameter with no value in the Via header field;

NOTE 2: When sending the unprotected REGISTER request using UDP, the UE transmit the request from the same IP address and port on which it expects to receive the response to this request.

e) a registration expiration interval value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and

   1) if GRUU is supported, the option-tag "gruu"; and

   2) if multiple registrations is supported, the option-tag "outbound".

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174].

NOTE 4: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

[TS 24.229, clause 5.1.1.2.6]

On sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field as defined in RFC 2617 shall not be included, in order to indicate support for GPRS-IMS-Bundled authentication.

b) the Security-Client header field as defined in RFC 3329 shall not be included;

c) a From header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003, as the public user identity to be registered;

d) a To header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003, as the public user identity to be registered;

e) the Contact header field with the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests; and

f) the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

NOTE 1: Since the private user identity is not included in the REGISTER requests when GPRS-IMS-Bundled authentication is used for registration, re-registration and de-registration procedures, all REGISTER requests from the UE use the IMSI-derived IMPU as the public user identity even when the implicitly registered IMPUs are available at the UE. The UE does not use the temporary public user identity (IMSI-derived IMPU) in any non-registration SIP requests.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.2.1, there are no additional requirements for the UE.

NOTE 2: When GPRS-IMS-Bundled authentication is in use, a 401 (Unauthorized) response to the REGISTER request is not expected to be received.

[TS 24.229, clause 5.1.1.3]

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the reg event package for the public user identity registered at the user's registrar (S-CSCF) as described in RFC 3680.

The UE shall subscribe to the reg event package upon registering a new contact address via an initial registration procedure. If the UE receives a NOTIFY request via the newly established subscription dialog and via the previously established subscription dialogs (there will be at least one), the UE may terminate the previously established subscription dialogs and keep only the newly established subscription dialog.

The UE shall use the default public user identity for subscription to the registration-state event package, if the public user identity that was used for initial registration is a barred public user identity. The UE may use either the default public user identity or the public user identity used for initial registration for the subscription to the registration-state event package, if the initial public user identity that was used for initial registration is not barred.

On sending a SUBSCRIBE request, the UE shall populate the header fields as follows:

a) a Request-URI set to the resource to which the UE wants to be subscribed to, i.e. to a SIP URI that contains the public user identity used for subscription;

b) a From header field set to a SIP URI that contains the public user identity used for subscription;

c) a To header field set to a SIP URI that contains the public user identity used for subscription;

d) an Event header field set to the "reg" event package;

e) an Expires header field set to 600 000 seconds as the value desired for the duration of the subscription;

f) void; and

g) void

[TS 24.229, clause 5.1.2A.1.1]

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

When the UE sends any request using a given contact address, the UE shall:

- if IMS AKA is in use as a security mechanism:

  a) if the UE has not obtained a GRUU, populate the Contact header field of the request with the protected server port and the respective contact address; and

  b) include the protected server port and the respective contact address in the Via header field entry relating to the UE;

…

- if GPRS-IMS-Bundled authentication is in use as a security mechanism, and therefore no port is provided for subsequent SIP messages by the P-CSCF during registration, the UE shall send any request to the same port used for the initial registration as described in subclause 5.1.1.2.

…

If this is a request for a new dialog, the Contact header field is populated as follows:

1) a contact header value which is one of:

   - if a public GRUU value ("pub-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does not indicate privacy of the P-Asserted-Identity, then the UE should insert the public GRUU ("pub-gruu" header field parameter) value as specified in RFC 5627; or

   - if a temporary GRUU value ("temp-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does indicate privacy of the P-Asserted-Identity, then the UE should insert the temporary GRUU ("temp-gruu" header field parameter) value as specified in RFC 5627; or

   - otherwise, a SIP URI containing the contact address of the UE;

   NOTE 7: The above items are mutually exclusive.

2) include an "ob" SIP URI parameter, if the UE supports multiple registrations, and the UE wants all subsequent requests in the dialog to arrive over the same flow identified by the flow token as described in RFC 5626;

3) if the request is related to an IMS communication service that requires the use of an ICSI then the UE shall include in a g.3gpp.icsi-ref media feature tag, as defined in subclause 7.9.2 and RFC 3841, the ICSI value (coded as specified in subclause 7.2A.8.2) for the IMS communication service. The UE may also include other ICSI values that the UE is prepared to use for all dialogs with the terminating UE(s); and

4) if the request is related to an IMS application that is supported by the UE, then the UE may include in a g.3gpp.iari-ref media feature tag, as defined in subclause 7.9.3 and RFC 3841, the IARI value (coded as specified in subclause 7.2A.9.2) that is related to the IMS application and that applies for the dialog.

…

If available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall insert a P-Access-Network-Info header field into any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method (see subclause 7.2A.4).

[TS 24.341, clause 5.3.2.2]

a) On sending a REGISTER request, the SM-over-IP receiver shall indicate its capability to receive traditional short messages over IMS network by including a "+g.3gpp.smsip" parameter into the Contact header according to RFC 3840.

Reference(s)

TS 24.229 [10] clauses 5.1.1.2.1, 5.1.1.2.6, 5.1.1.3, 5.1.2A.1.2 and TS 24.341 [90] clause 5.3.2.2.

8.10.3 Test purpose

1) To verify that UE correctly derives a temporary public user identity from the IMSI parameter.

2) To verify that UE correctly derives a home network domain name from the IMSI parameter.

3) To verify that the UE sends a correctly composed initial REGISTER request.

4) To verify that after receiving a 200 OK response, the UE subscribes to the reg event package.

5) To verify that the UE responds the received NOTIFY with 200 OK.

8.10.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services, but has an active PDP context and has discovered the SS as P-CSCF by executing the generic test procedure in Annex C.2a up to step 3.

SS is configured with the IMSI, the home domain name, public and private user identities and the currently assigned IP address. SS is listening to SIP default port 5060 for both UDP and TCP protocols.

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

GIBA (Yes/No)

obtaining and using GRUUs in the Session Initiation Protocol (SIP) (Yes/No)

UE supports MTSI (Yes/No)

UE supports SM-over-IP receiver (Yes/No)

Test procedure

1) The UE initiates IMS registration indicating support of GIBA. SS waits for the UE to send an initial REGISTER request.

2) The SS responds to the REGISTER request with a 200 OK response,

3) The SS waits for the UE to send a SUBSCRIBE request.

4) The SS responds to the SUBSCRIBE request with a 200 OK response.

5) The SS sends a valid NOTIFY request for the subscribed registration event package.

6) The SS waits for the UE to respond to the NOTIFY with a 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	The UE sends initial registration for IMS services indicating support for GIBA procedure by not including an Authorization header field.
2	←		200 OK	The SS responds with 200 OK.
3	→		SUBSCRIBE	The UE subscribes to its registration event package.
4	←		200 OK	The SS responds with 200 OK.
5	←		NOTIFY	The SS sends initial NOTIFY for registration event package, containing full registration state information for the registered public user identity in the XML body
6	→		200 OK	The UE responds with 200 OK.

NOTE: The default message contents in annex A are used.

Specific Message Contents

REGISTER (Step 1)

Use the default message 'REGISTER' in annex A.1.1 with condition A3 "REGISTER for the case UE supports GIBA" and condition A6 'The UE supports SM-over-IP receiver' (if UE supports SM-over-IP receiver marked as yes).

200 OK for REGISTER (Step 2)

Use the default message '200 OK for REGISTER' in annex A.1.3 with condition A2 'GIBA'.

SUBSCRIBE (Step 3)

Use the default message 'SUBSCRIBE for reg-event package' in annex A.1.4 with condition A2 'GIBA'.

200 OK for SUBSCRIBE (Step 4)

Use the default message '200 OK for SUBSCRIBE' in annex A.1.5 with condition A2 'GIBA'.

NOTIFY (Step 5)

Use the default message 'NOTIFY for reg-event package' in annex A.1.6 with condition A2 'GIBA'.

200 OK for NOTIFY (Step 6)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

8.10.5 Test requirements

The UE shall send requests and responses as described in clause 8.10.4.

8.11 Initial registration using IMS AKA and GIBA against a network with GIBA support only

8.11.1 Definition and applicability

Test to verify that the UE can correctly register to IMS services in a network with support for GIBA only, when equipped with UICC that contains either both ISIM and USIM applications or only USIM application but not ISIM. The process consists of sending initial registration to S-CSCF via the P-CSCF discovered, authenticating the user and finally subscribing the registration event package for the registered default public user identity. The test case is applicable when both IMS security and GIBA are supported.

8.11.2 Conformance requirement

[TS 24.229, clause 5.1.1.2.1]

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B. A public user identity may be input by the end user.

On sending an unprotected REGISTER request, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) containing the IP address or FQDN of the UE in the hostport parameter. If the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations, the UE shall include a "+sip.instance" header field parameter containing the instance ID. If the UE supports multiple registrations it shall include "reg-id" header field parameter as described in RFC 5626. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 for the IMS communication services it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840;

d) a Via header field set to include the sent-by field containing the IP address or FQDN of the UE and the port number where the UE expects to receive the response to this request when UDPis used. For TCP, the response is received on the TCP connection on which the request was sent. For the UDP, the UE shall also include a "rport" header field parameter with no value in the Via header field;

NOTE 2: When sending the unprotected REGISTER request using UDP, the UE transmit the request from the same IP address and port on which it expects to receive the response to this request.

e) a registration expiration interval value of 600 000 seconds as the value desired for the duration of the registration;

NOTE 3: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and

1) if GRUU is supported, the option-tag "gruu"; and

2) if multiple registrations is supported, the option-tag "outbound".

h) if a security association or TLS session exists, and if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174].

NOTE 4: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

[TS 24.229, clause 5.1.1.2.2]

On sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field, with:

- the "username" header field parameter, set to the value of the private user identity;

- the "realm" header field parameter, set to the domain name of the home network;

- the "uri" header field parameter, set to the SIP URI of the domain name of the home network;

- the "nonce" header field parameter, set to an empty value; and

- the "response" header field parameter, set to an empty value;

NOTE 1: If the UE specifies its FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security association. For details on the selection of the port values see 3GPP TS 33.203.

b) additionally for the Contact header field, if the REGISTER request is protected by a security association, include the protected server port value in the hostport parameter;

c) additionally for the Via header field, for UDP, if the REGISTER request is protected by a security association, include the protected server port value in the sent-by field; and

d) a Security-Client header field set to specify the signalling plane security mechanism the UE supports, the IPsec layer algorithms the UE supports and the parameters needed for the security association setup. The UE shall support the setup of two pairs of security associations as defined in 3GPP TS 33.203. The syntax of the parameters needed for the security association setup is specified in annex H of 3GPP TS 33.203. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329. The UE shall support the IPsec layer algorithms for integrity and confidentiality protection as defined in 3GPP TS 33.203, and shall announce support for them according to the procedures defined in RFC 3329.

[TS 24.229, clause 5.1.1.2.6]

On sending a REGISTER request, as defined in subclause 5.1.1.2.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field as defined in RFC 2617 shall not be included, in order to indicate support for GPRS-IMS-Bundled authentication.

b) the Security-Client header field as defined in RFC 3329 shall not be included;

c) a From header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003, as the public user identity to be registered;

d) a To header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003, as the public user identity to be registered;

e) the Contact header field with the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests; and

f) the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

NOTE 1: Since the private user identity is not included in the REGISTER requests when GPRS-IMS-Bundled authentication is used for registration, re-registration and de-registration procedures, all REGISTER requests from the UE use the IMSI-derived IMPU as the public user identity even when the implicitly registered IMPUs are available at the UE. The UE does not use the temporary public user identity (IMSI-derived IMPU) in any non-registration SIP requests.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.2.1, there are no additional requirements for the UE.

NOTE 2: When GPRS-IMS-Bundled authentication is in use, a 401 (Unauthorized) response to the REGISTER request is not expected to be received.

[TS 24.229, clause 5.1.1.3]

Upon receipt of a 2xx response to the initial registration, the UE shall subscribe to the reg event package for the public user identity registered at the user's registrar (S-CSCF) as described in RFC 3680.

The UE shall subscribe to the reg event package upon registering a new contact address via an initial registration procedure. If the UE receives a NOTIFY request via the newly established subscription dialog and via the previously established subscription dialogs (there will be at least one), the UE may terminate the previously established subscription dialogs and keep only the newly established subscription dialog.

The UE shall use the default public user identity for subscription to the registration-state event package, if the public user identity that was used for initial registration is a barred public user identity. The UE may use either the default public user identity or the public user identity used for initial registration for the subscription to the registration-state event package, if the initial public user identity that was used for initial registration is not barred.

On sending a SUBSCRIBE request, the UE shall populate the header fields as follows:

a) a Request-URI set to the resource to which the UE wants to be subscribed to, i.e. to a SIP URI that contains the public user identity used for subscription;

b) a From header field set to a SIP URI that contains the public user identity used for subscription;

c) a To header field set to a SIP URI that contains the public user identity used for subscription;

d) an Event header field set to the "reg" event package;

e) an Expires header field set to 600 000 seconds as the value desired for the duration of the subscription;

f) void; and

g) void

[TS 24.229, clause 5.1.2A.1.1]

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

When the UE sends any request using a given contact address, the UE shall:

- if IMS AKA is in use as a security mechanism:

  a) if the UE has not obtained a GRUU, populate the Contact header field of the request with the protected server port and the respective contact address; and

  b) include the protected server port and the respective contact address in the Via header field entry relating to the UE;

…

- if GPRS-IMS-Bundled authentication is in use as a security mechanism, and therefore no port is provided for subsequent SIP messages by the P-CSCF during registration, the UE shall send any request to the same port used for the initial registration as described in subclause 5.1.1.2.

…

If this is a request for a new dialog, the Contact header field is populated as follows:

1) a contact header value which is one of:

   - if a public GRUU value ("pub-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does not indicate privacy of the P-Asserted-Identity, then the UE should insert the public GRUU ("pub-gruu" header field parameter) value as specified in RFC 5627; or

   - if a temporary GRUU value ("temp-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does indicate privacy of the P-Asserted-Identity, then the UE should insert the temporary GRUU ("temp-gruu" header field parameter) value as specified in RFC 5627; or

   - otherwise, a SIP URI containing the contact address of the UE;

   NOTE 7: The above items are mutually exclusive.

2) include an "ob" SIP URI parameter, if the UE supports multiple registrations, and the UE wants all subsequent requests in the dialog to arrive over the same flow identified by the flow token as described in RFC 5626;

3) if the request is related to an IMS communication service that requires the use of an ICSI then the UE shall include in a g.3gpp.icsi-ref media feature tag, as defined in subclause 7.9.2 and RFC 3841, the ICSI value (coded as specified in subclause 7.2A.8.2) for the IMS communication service. The UE may also include other ICSI values that the UE is prepared to use for all dialogs with the terminating UE(s); and

4) if the request is related to an IMS application that is supported by the UE, then the UE may include in a g.3gpp.iari-ref media feature tag, as defined in subclause 7.9.3 and RFC 3841, the IARI value (coded as specified in subclause 7.2A.9.2) that is related to the IMS application and that applies for the dialog.

…

If available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall insert a P-Access-Network-Info header field into any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method (see subclause 7.2A.4).

[TS 33.203, clause T.7]

3. ME supports both, IMS network supports GIBA security only.

   The ME shall check the smartcard application in use.

   If a SIM is in use, then it shall start with a GIBA security procedure, else it shall start with the fully compliant IMS Registration procedure.

   In the second case, the GIBA P-CSCF shall answer with a 420 (Bad Extension) failure, since it does not recognize the method mandated by the Proxy-Require header that is sent by the UE in the initial REGISTER request.

NOTE 2: The Proxy-Require header cannot be ignored by the P-CSCF.

The UE shall, after receiving the error response, send a GIBA registration, i.e., shall send a new REGISTER request without the fully compliant IMS security headers.

NOTE 3: If the UE already has knowledge about the IMS network capabilities (which could for example be preconfigured in the UE), the appropriate authentication method can be chosen. The UE can use fully compliant IMS security, if the network supports this, otherwise the UE can use GIBA security.

[TS 24.341, clause 5.3.2.2]

b) On sending a REGISTER request, the SM-over-IP receiver shall indicate its capability to receive traditional short messages over IMS network by including a "+g.3gpp.smsip" parameter into the Contact header according to RFC 3840.

Reference(s)

TS 24.229 [10] clauses 5.1.1.2.1, 5.1.1.2.2, 5.1.1.2.6, 5.1.1.3, 5.1.2A.1.2, TS 33.203 [14] clause T.7 and TS 24.341 [90] clause 5.3.2.2.

8.11.3 Test purpose

1) To verify that UE correctly derives a private user identity, a temporary public user identity and a home network domain name from the IMSI parameter in the USIM or alternatively use the values retrieved from ISIM.

2) To verify that the UE sends a correctly composed initial REGISTER request.

3) To verify that after receiving a 420 (Bad Extension) response the UE sends a correctly composed initial REGISTER request.

4) To verify that after receiving a 200 OK response, the UE subscribes to the reg event package.

5) To verify that the UE responds the received NOTIFY with 200 OK.

8.11.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services, but has an active PDP context and has discovered the SS as P-CSCF by executing the generic test procedure in Annex C.2 up to step 3. The UE has no knowledge about the IMS network capabilities.

SS is configured with the IMSI, the home domain name, public and private user identities and the currently assigned IP address. SS is listening to SIP default port 5060 for both UDP and TCP protocols.

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

GIBA (Yes/No)

obtaining and using GRUUs in the Session Initiation Protocol (SIP) (Yes/No)

UE supports MTSI (Yes/No)

UE supports SM-over-IP receiver (Yes/No)

Test procedure

1) IMS registration is initiated on the UE. SS waits for the UE to send an initial REGISTER request.

2) The SS responds to the REGISTER request with a 420 Bad Extension response,

3) The UE initiates IMS registration indicating support of early IMS security. SS waits for the UE to send an initial REGISTER request.

4) The SS responds to the REGISTER request with valid 200 OK response,

5) The SS waits for the UE to send a SUBSCRIBE request.

6) The SS responds to the SUBSCRIBE request with a valid 200 OK response.

7) The SS sends a NOTIFY request for the subscribed registration event package.

8) The SS waits for the UE to respond to the NOTIFY with a 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE sends initial registration for IMS services.
2	←		420 Bad Extension	The SS responds with a failure, since the option tag sec-agree in the Proxy-Require header field is not supported.
3	→		REGISTER	The UE sends initial registration for IMS services indicating support for GIBA procedure by not including an Authorization header field.
4	←		200 OK	The SS responds with 200 OK.
5	→		SUBSCRIBE	The UE subscribes to its registration event package.
6	←		200 OK	The SS responds with 200 OK.
7	←		NOTIFY	The SS sends initial NOTIFY for registration event package, containing full registration state information for the registered public user identity in the XML body
8	→		200 OK	The UE responds with 200 OK.

NOTE: The default message contents in annex A are used.

Specific Message Contents

REGISTER (Step 1)

Use the default message 'REGISTER' in annex A.1.1 with condition A1 "Initial unprotected REGISTER" and condition A6 'The UE supports SM-over-IP receiver' (if UE supports SM-over-IP receiver marked as yes)

420 Bad Extension (Step 2)

Use the default message '420 Bad Extension for REGISTER' in annex A.1.8

REGISTER (Step 3)

Use the default message 'REGISTER' in annex A.1.1 with condition A3 "REGISTER for the case UE supports GIBA" and condition A6 'The UE supports SM-over-IP receiver' (if UE supports SM-over-IP receiver marked as yes)

200 OK for REGISTER (Step 4)

Use the default message '200 OK for REGISTER' in annex A.1.3 with condition A2 'GIBA'

SUBSCRIBE (Step 5)

Use the default message 'SUBSCRIBE for reg-event package' in annex A.1.4 with condition A2 'GIBA'.

200 OK for SUBSCRIBE (Step 6)

Use the default message '200 OK for SUBSCRIBE' in annex A.1.5 with condition A2 'GIBA'

NOTIFY (Step 7)

Use the default message 'NOTIFY for reg-event package' in annex A.1.6 with condition A2 'GIBA'

200 OK for NOTIFY (Step 8)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

8.11.5 Test requirements

The UE shall send requests and responses as described in clause 8.11.4.

8.12 User initiated re-registration using GIBA

8.12.1 Definition and applicability

Test to verify that the UE can re-register a previously registered public user identity at any time. The test case is applicable for UE supporting GIBA only.

8.12.2 Conformance requirement

[TS 24.229, clause 5.1.1.4.1]

The UE can perform the reregistration of a previously registered public user identity bound to any one of its contact addresses and the associated set of security associations or TLS sessions at any time after the initial registration has been completed.

The UE can perform the reregistration of a previously registered public user identity over any existing set of security associations or TLS session that is associated with the related contact address.

…

Unless either the user or the application within the UE has determined that a continued registration is not required the UE shall reregister an already registered public user identity either 600 seconds before the expiration time if the previous registration was for greater than 1200 seconds, or when half of the time has expired if the previous registration was for 1200 seconds or less, or when the UE intends to update its capabilities according to RFC 3840 or when the UE needs to modify the ICSI values that the UE intends to use in a g.3gpp.icsi-ref media feature tag or IARI values that the UE intends to use in the g.3gpp.iari-ref media feature tag.

…

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) that contain(s) in the hostport parameter the IP address or FQDN of the UE, and containing the instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations. If the UE support multiple registrations, it shall include "reg-id" header field as described in RFC 5626. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 for the IMS communication it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840;

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field. For the TCP, the response is received on the TCP connection on which the request was sent;

e) a registration expiration interval value, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 1: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and if GRUU is supported, the option-tag "gruu";

h) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter.

NOTE 2: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) bind the new expiration time of the registration for this public user identity found in the To header field value to the contact address used in this registration;

[TS 24.229, clause 5.1.1.4.6]

On sending a REGISTER request, as defined in subclause 5.1.1.4.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field as defined in RFC 2617 shall not be included, in order to indicate support GPRS-IMS-Bundled authentication.

b) security agreement header field values as required by RFC 3329 shall not contain signalling plane security mechanisms;

c) a From header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003, as the public user identity to be registered;

d) a To header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003, as the public user identity to be registered;

e) the Contact header field with the port value of an unprotected port where the UE expects to receive subsequent mid-dialog requests; and

f) the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

NOTE 1: Since the private user identity is not included in the REGISTER requests when GPRS-IMS-Bundled authentication is used for registration, re-registration and de-registration procedures, all REGISTER requests from the UE use the IMSI-derived IMPU as the public user identity even when the implicitly registered IMPUs are available at the UE. The UE does not use the temporary public user identity (IMSI-derived IMPU) in any non-registration SIP requests.

On receiving the 200 (OK) response to the REGISTER request defined in subclause 5.1.1.4.1, there are no additional requirements for the UE.

NOTE 2: When GPRS-IMS-Bundled authentication is in use, a 401 (Unauthorized) response to the REGISTER request is not expected to be received.

[TS 24.341, clause 5.3.2.2]

c) On sending a REGISTER request, the SM-over-IP receiver shall indicate its capability to receive traditional short messages over IMS network by including a "+g.3gpp.smsip" parameter into the Contact header according to RFC 3840.

Reference(s)

TS 24.229 [10] clauses 5.1.1.4.1, 5.1.1.4.6 and TS 24.341 [90] clause 5.3.2.2.

8.12.3 Test purpose

1) To verify that the UE can re-register a previously registered public user identity at either 600 seconds before the expiration time if the initial registration was for greater than 1200 seconds, or when half of the time has expired if the initial registration was for 1200 seconds or less.

2) Upon receiving 200 OK for REGISTER, the UE shall store the new expiration time of the registration for this public user identity.

8.12.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services. Execute the generic test procedure in annex C.2a up to step 3.

SS is configured with the IMSI, the home domain name, public and private user identities and the currently assigned IP address. SS is listening to SIP default port 5060 for both UDP and TCP protocols.

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

GIBA (Yes/No)

obtaining and using GRUUs in the Session Initiation Protocol (SIP) (Yes/No)

UE supports MTSI (Yes/No)

UE supports SM-over-IP receiver (Yes/No)

Test procedure

1-6) The same procedure as in subclause 8.10.4 are used with the exception that the SS sets the expiration time to 120 seconds in Step 4.

7) Before half of the time has expired from the initial registration SS receives re-register message request with the From, To, Via, Contact, Expires, Supported, and P-Access-Network-Info header fields.

8) SS responds to the REGISTER request with valid 200 OK response with the list of URIs contained in the P-Associated-URI header value, the new expiration time (1200 seconds) of the registration for this public user identity.

9) SS waits for the REGISTER request and verifies it is received at least 600 seconds before the expected expiration time.

10) SS responds to the REGISTER request with valid 200 OK response with the list of URIs contained in the P-Associated-URI header value, the new expiration time (1800 seconds) of the registration for this public user identity.

11) SS waits for the REGISTER request and verifies it is received at least 600 seconds before the expected expiration time.

12) SS responds to the REGISTER request with valid 200 OK response. SS shall populate the headers of the 200 OK response according to the 200 response for REGISTER common message definition.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-6			Messages in Initial Registration Test case (subclause 8.10.4)	The same messages as in subclause 8.10.4 are used with the exception that in Step 4, the SS responds with 200 OK indicating 120 seconds expiration time.
7	→		REGISTER	The SS receives REGISTER from the UE 60 seconds before the expiration time set in the initial registration request.
8	←		200 OK	The SS responds with 200 OK indicating 1200 seconds expiration time.
9	→		REGISTER	The SS receives REGISTER from the UE 600 seconds before the expiration time set in step 8.
10	←		200 OK	The SS responds with 200 OK indicating 1800 seconds expiration time.
11	→		REGISTER	The SS receives REGISTER from the UE 600 seconds before the expiration time set in step 10
12	←		200 OK	The SS responds with 200 OK indicating the default expiration time.

Specific Message Contents

Messages in Step 1-6

Messages in Step 1-6 are the same as those specified in subclause 8.10.4 with the following exception for the 200 OK for REGISTER in Step 4:

Use the default message '200 OK for REGISTER' in annex A.1.3 with the following exceptions:

Header/param	Value/remark
Contact	
expires	120

REGISTER (Step 7)

Use the default message 'REGISTER' in annex A.1.1 with condition A3 'REGISTER for the case UE supports GIBA' and condition A6 'The UE supports SM-over-IP receiver' (if UE supports SM-over-IP receiver marked as yes).

200 OK for REGISTER (Step 8)

Use the default message '200 OK for REGISTER' in annex A.1.3 with the following exceptions:

Header/param	Value/remark
Contact	
expires	1200

REGISTER (Step 9)

Use the default message 'REGISTER' in annex A.1.1 with condition A3 'REGISTER for the case UE supports GIBA' and condition A6 'The UE supports SM-over-IP receiver' (if UE supports SM-over-IP receiver marked as yes).

200 OK for REGISTER (Step 10)

Use the default message '200 OK for REGISTER' in annex A.1.3 with the following exceptions:

Header/param	Value/remark
Contact	
expires	1800

REGISTER (Step 11)

Use the default message 'REGISTER' in annex A.1.1 with condition A3 'REGISTER for the case UE supports GIBA' and condition A6 'The UE supports SM-over-IP receiver' (if UE supports SM-over-IP receiver marked as yes).

200 OK for REGISTER (Step 12)

Use the default message '200 OK for REGISTER' in annex A.1.3.

8.12.5 Test requirements

The UE shall send requests and responses as described in clause 8.12.4

8.13 User initiated de-registration using GIBA

8.13.1 Definition and applicability

Test to verify that the UE can perform a correct de-registration procedure. The test case is applicable for UE supporting GIBA only.

8.13.2 Conformance requirement

[TS 24.229, clause 5.1.1.6.1]

The UE can deregister a public user identity that it has previously registered with its contact address at any time.

…

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B.

…

On sending a REGISTER request that will remove the binding between the public user identity and one of its contact addresses, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be deregistered;

b) a To header field set to the SIP URI that contains the public user identity to be deregistered;

c) a Contact header field set to the SIP URI(s) that contain(s) in the hostport parameter the IP address of the UE or FQDN, and containing the Instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations. If the UE supports multiple registrations, it shall include "reg-id" header field parameter as described in RFC 5626;

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field;

e) a registration expiration interval value set to the value of zero, appropriate to the deregistration requirements of the user;

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

h) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter.

NOTE 1: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

For a public user identity that the UE has registered with multiple contact addresses (e.g. via different P-CSCFs), the UE shall also be able to deregister multiple contact addresses, bound to its public user identity, via single deregistration procedure as specified in RFC 3261. The UE shall send a single REGISTER request, using one of its contact addresses and the associated set of security associations or TLS session, containing a list of Contact headers. Each Contact header in the list shall contain the contact addresses that the UE wants to deregister with the "expires" parameter containing the value equal zero.

The UE can deregister all contact addresses bound to its public user identity and associated with its private user identity. The UE shall send a single REGISTER request, using one of its contact addresses and the associated set of security associations or TLS session, containing a public user identity that is being deregistered in the To header field, and a single Contact header field with value of "*" and the Expires header field with a value of "0".

NOTE 2: All entities subscribed to the reg event package of the user will be inform via NOTIFY request which contact addresses bound to the public user identity have been deregistered.

[TS 24.229, clause 5.1.1.6.6]

On sending a REGISTER request, as defined in subclause 5.1.1.6.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field as defined in RFC 2617 shall not be included, in order to indicate support GPRS-IMS-Bundled authentication.

b) the Security-Verify header field and the Security-Client header field values as defined by RFC 3329 shall not contain signalling plane security mechanisms;

c) a From header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003, as the public user identity to be deregistered;

d) a To header field set to a temporary public user identity derived from the IMSI, as defined in 3GPP TS 23.003, as the public user identity to be deregistered;

e) for each Contact header field and associated contact address include the associated unprotected port value (where the UE was expecting to receive mid-dialog requests); and

f) the Via header field with the port value of an unprotected port where the UE expects to receive responses to the request.

NOTE 1: Since the private user identity is not included in the REGISTER requests when GPRS-IMS-Bundled authentication is used for registration, re-registration and de-registration procedures, all REGISTER requests from the UE use the IMSI-derived IMPU as the public user identity even when the implicitly registered IMPUs are available at the UE. The UE does not use the temporary public user identity (IMSI-derived IMPU) in any non-registration SIP requests.

[TS 24.341, clause 5.3.2.2]

c) On sending a REGISTER request, the SM-over-IP receiver shall indicate its capability to receive traditional short messages over IMS network by including a "+g.3gpp.smsip" parameter into the Contact header according to RFC 3840.

Reference(s)

TS 24.229 [10] clauses 5.1.1.6.1, 5.1.1.6.6 and TS 24.341 [90] clause 5.3.2.2.

8.13.3 Test purpose

1) To verify that the UE sends an initial REGISTER request with an expiration interval value set to 0.

8.13.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. Execute the generic test procedure in annex C.2a.

SS is configured with the IMSI, the home domain name, public and private user identities and the currently assigned IP address. SS is listening to SIP default port 5060 for both UDP and TCP protocols.

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

GIBA (Yes/No

obtaining and using GRUUs in the Session Initiation Protocol (SIP) (Yes/No)

UE supports MTSI (Yes/No)

UE supports SM-over-IP receiver (Yes/No)

Test procedure

1) The UE is triggered by MMI to initiate a deregistration procedure

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE sends deregistration for IMS services.
2	←		200 OK	The SS responds REGISTER with 200 OK

Specific message contents

REGISTER (step 1)

Use the default message 'REGISTER' in annex A.1.1 with condition A3 "REGISTER for the case UE supports GIBA" and condition A6 'The UE supports SM-over-IP receiver' (if UE supports SM-over-IP receiver marked as yes) with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	SIP URI with IP address or FQDN and unprotected server port of UE or *
expires	*0* (if present)
Expires	(must be present if addr-spec is *)
delta-seconds	*0* (if present)
Supported	header may be missing or it may contain any value

8.13.5 Test requirements

The UE shall send requests and responses as described in clause 8.13.4

8.14 Initial registration for three implicit registration sets

8.14.1 Definition and applicability

Test to verify that the UE can correctly register to IMS services when equipped with UICC that contains ISIM application with multiple IMS public user identities (IMPU) belonging to three different implicit registration sets. Test case verifies that the UE is able to register the registration sets on parallel. The test case is applicable for IMS security.

8.14.2 Conformance requirement

[TS 24.229, clause 5.1.1.1A]:

The ISIM shall always be used for authentication to the IM CN subsystem, if it is present, as described in 3GPP TS 33.203.

The ISIM is preconfigured with all the necessary parameters to initiate the registration to the IM CN subsystem. These parameters include:

- the private user identity;
- one or more public user identities; and
- the home network domain name used to address the SIP REGISTER request

The first public user identity in the list stored in the ISIM is used in emergency registration requests.

[TS 24.229, clause 5.1.1.2.1]:

The initial registration procedure consists of the UE sending an unprotected REGISTER request and, if challenged depending on the security mechanism supported for this UE, sending the integrity-protected REGISTER request or other appropriate response to the challenge. The UE can register a public user identity with any of its contact addresses at any time after it has acquired an IP address, discovered a P-CSCF, and established an IP-CAN bearer that can be used for SIP signalling. However, the UE shall only initiate a new registration procedure when it has received a final response from the registrar for the ongoing registration, or the previous REGISTER request has timed out.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.1.1A and 5.1.1.2.1

8.14.3 Test purpose

1) To verify that UE is able to register three different IMS public user identities (IMPU), as found from ISIM, belonging to three different implicit registration sets.

8.14.4 Method of test

Initial conditions

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE is equipped with a UICC that contains both ISIM and USIM applications. UE is not registered to IMS services, but has an active PDP context/ established EPS default bearer context and has discovered the SS as P-CSCF by executing the generic test procedure in Annex C.2 up to step 3.

Related ICS/IXIT Statement(s)

- UE supports IPSec ESP confidentiality protection (Yes/No)

- IMS security (Yes/No)
- obtaining and using GRUUs in the Session Initiation Protocol (SIP) (Yes/No)
- UE supports MTSI (Yes/No)
- UE supports automatic consecutive registration of multiple SIP URI IMPUs stored on the ISIM (belonging to separate implicit registration sets) (Yes/No)
- UE supports manual registration of multiple SIP URIs IMPUs stored on the ISIM (belonging to separate implicit registration sets) (Yes/No)

Test procedure

1) If the UE supports automatic consecutive registration of multiple SIP URI IMPUs the UE is made to register all implicit registration sets for the IMPUs found on ISIM otherwise if the supports manual registration of multiple SIP URIs IPMUs the UE is triggered to register one of the SIP URI IMPUs.
2) The UE executes the procedures of annex C.2 for context activation and subsequent IMS registration. The registration event sent by the SS indicates only that IMPU to have been registered, which was explicitly registered by the UE.
3) If the UE does not support automatic consecutive registration of multiple SIP URI IMPUs and supports manual registration of multiple SIP URIsIMPUs the UE is triggered to register another SIP URI IMPU.
4) The UE initiates another registration procedure of annex C.23, in order to register a second implicit registration set. The registration event sent by the SS indicates the rest of the two IMPUs within ISIM to have been registered.
5) If the UE does not support automatic consecutive registration of multiple SIP URI IMPUs and supports manual registration of multiple SIP URIs IMPUs the UE is triggered to register a third SIP URI IMPU.
6) The UE initiates a third registration procedure of annex C.23, in order to register a third implicit registration set. The registration event sent by the SS indicates all the three IMPUs within ISIM to have been registered.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1				Registration of first IMPU is triggered either automatically or manually.
2			Steps defined in annex C.2	EPS bearer or PDP context activation and subsequent IMS registration for the first implicit registration set by the UE
3				Registration of second IMPU is triggered either automatically or manually.
4			Steps defined in annex C.23	IMS registration for the second implicit registration set
5				Registration of second IMPU is triggered either automatically or manually.
6			Steps defined in annex C.23	IMS registration for the third implicit registration set

Specific Message Contents

NOTIFY (within step 2)

Use the default message 'NOTIFY for reg-event package' in annex A.1.6 with the following exceptions:

Header/param	*Cond*	Value/remark	Rel	Reference
Message-body	A3	<?xml version='1.0?> <reginfo xmlns='urn:ietf:params:xml:ns:reginfo' version='0' state='full'> <registration aor='<IMPU registered by the UE>' id='a100' state='active'> <contact id='980' state='active' event='registered'> <uri>same value as in Contact header of REGISTER request</uri> </contact> </reginfo>		RFC 3680 [22]
	A4	<?xml version='1.0?> <reginfo xmlns='urn:ietf:params:xml:ns:reginfo' xmlns:gr="urn:ietf:params:xml:ns:gruuinfo" version='0' state='full'> <registration aor='<IMPU registered by the UE>' id='a100' state='active'> <contact id='980' state='active' event='registered' callid="Call-Id of most recent REGISTER" cseq="CSeq value of most recent REGISTER"> <uri>same value as in Contact header of REGISTER request</uri> <allOneLine> <unknown-param name="+sip.instance"> "Instance ID of the UE;" </unknown-param> </allOneLine> <allOneLine> <gr:pub-gruu uri="public GRUU for the UE"/> </allOneLine> <allOneLine> <gr:temp-gruu uri="temporary GRUU for the UE" first-cseq="CSeq of the REGISTER request that caused the temporary GRUU to assigned for the UE"/> </allOneLine> </contact> </registration> </reginfo>		draft-ietf-sipping-gruu-reg-event [62]

NOTIFY (within step 4)

Use the default message 'NOTIFY for reg-event package' in annex A.1.6 with the following exceptions:

- The version of the reginfo to be 1 instead of 0.
- The state of the reginfo to be 'partial' instead of 'full'
- Within the reginfo XML structure there is only one single <registration> element for the IMPU registered within step 4 by the UE

NOTIFY (within step 6)

Use the default message 'NOTIFY for reg-event package' in annex A.1.6 with the following exceptions:

- The version of the reginfo to be 2 instead of 0.
- The state of the reginfo to be 'partial' instead of 'full'.
- Within the reginfo XML structure there is only one single <registration> element for the IMPU registered within step 6 by the UE.

Thus:

- The full registration event sent by SS after the first REGISTER from the UE indicates only single IMPU explicitly registered to belong to the first implicit registration set.

- The partial event sent by SS after the second REGISTER from the UE indicates second IMPUs on ISIM to have been registered.
- The partial event sent by SS after the third REGISTER from the UE indicates the third IMPUs on ISIM to have been registered.

8.14.5 Test requirements

UE shall register three implicit registration sets to which the IMPUs on ISIM have been divided.

The UE shall read the following parameters from ISIM and use them for the REGISTER requests:

- the private user identity; and
- the public user identities; and
- the home network domain name.

8.15 Refresh for ISIM parameters

8.15.1 Definition and applicability

Test to verify that the when ISIM parameter values have been updated the UE will use the new values when registering to IMS the next time.

8.15.2 Conformance requirement

[TS 24.229 Annex C.4]:

The 3GPP TS 31.102 and 3GPP TS 31.103 specify the file structure and contents for the preconfigured parameters stored on the USIM and ISIM, respectively, necessary to initiate the registration to the IM CN subsystem. Any of these parameters can be updated via Data Download or a USAT application, as described in 3GPP TS 31.111. If one or more EFs are changed and a REFRESH command is issued by the UICC, then the UE reads the updated parameters from the UICC as specified for the REFRESH command in 3GPP TS 31.111.

In case of changes to EFs, the UE is not required to perform deregistration but it shall wait for the network-initiated deregistration procedures to occur as described in subclause 5.4.1.5 unless the user initiates deregistration procedures as described in subclause 5.1.1.6. From this point onwards the normal initial registration procedures can occur.

[TS 24.229 clause 5.1.1.7]:

Upon receipt of a NOTIFY request on any dialog which was generated during subscription to the reg event package as described in subclause 5.1.1.3, including one or more <registration> element(s) which were registered by this UE with:

- the state attribute set to "terminated" and the event attribute within the <contact> element belonging to this UE set to "rejected" or "deactivated"; or
- the state attribute set to "active" and within the <contact> element belonging to this UE, the state attribute set to "terminated" and the associated event attribute set to "rejected" or "deactivated";

the UE shall remove all registration details relating to these public user identities. In case of a "deactivated" event attribute, the UE shall start the initial registration procedure as described in subclause 5.1.1.2.

Reference(s)

3GPP TS 24.229[10], clause 5.1.1.7, annex C.4 (release 10)

8.15.3 Test purpose

1) To verify that the update of ISIM parameters related to IMS registration (and consequent REFRESH command) does not cause the UE to immediately deregister from IMS; and

2) To verify that the UE uses the updated parameter values from ISIM when registering to IMS again after the network initiated deregistration procedure

8.15.4 Method of test

Initial conditions

SS is configured with the old and new home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE is equipped with a UICC that contains both ISIM and USIM applications. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step. The Request-URI of SIP REGISTER request sent by the UE contained the old home domain name and IMS identities as found from ISIM.

Related ICS/IXIT Statement(s)

- IMS security (Yes/No)

Test procedure

1) The UICC is made to send a REFRESH command to the UE indicating that contents of ISIM has been updated.

NOTE: The specific way to trigger the REFRESH command is a test implementation option.

2) 10 seconds after step 1 SS sends a SIP NOTIFY request in order to terminate the IMS registration.

3) UE responds the NOTIFY request with 200 OK response.

4) UE initiates a new IMS registration sequence. For SIP REGISTER request the UE uses the new values of home domain name and/or IMS identities as provided by ISIM after the update.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			REFRESH	The UICC is made to send a REFRESH command to the UE indicating that contents of ISIM has been updated.
2	←		NOTIFY	10 seconds after previous step 1 the SS sends SIP NOTIFY for registration event package, containing full registration state information, with all previously registered IMS public user identities as "terminated" and "deactivated"
3	→		200 OK	The UE responds the NOTIFY with 200 OK
4			Steps defined in annex C.2 from step 4 onwards	UE initiates a new IMS registration sequence. For the Request-URI of SIP REGISTER request the UE uses the new value of home domain and/or IMS identities name as provided by ISIM after the update in step 1.

Specific Message Contents

NOTIFY (Step 2)

Use the default message 'NOTIFY for reg-event package' in annex A.1.6 with the following exceptions:

Header/param	Value/remark
CSeq	
value	2
Subscription-State	
substate-value	*Terminated*
expires	*0*
Message-body	*<?xml version='1.0?>* *<reginfo xmlns='urn:ietf:params:xml:ns:reginfo' version='1' state='full'>* *<registration aor=*'PublicUserIdentity1 (NOTE 1)' *id='a100' state='terminated'>* *<contact id='980' state='terminated' event='deactivated'>* <*uri*>same value as in Contact header of REGISTER request*</uri>* *</contact>* *</registration>* *<registration aor=*'AssociatedTelUri (NOTE 1)' *id='a101' state='terminated'>* *<contact id='981' state='terminated' event='deactivated'>* <*uri*>same value as in Contact header of REGISTER request*</uri>* *</contact>* *</registration>* *<registration aor=*'PublicUserIdentity2 (NOTE 1)' *id='a102' state='terminated'>* *<contact id='982' state='terminated' event='deactivated'>* <*uri*>same value as in Contact header of REGISTER request*</uri>* *</contact>* *</registration>* *</reginfo>*

NOTE 1: The public user ids and the associated TEL URI are as returned to the UE in the P-Associated-URI header of the 200 (OK) response to the REGISTER request;
PublicUserId1 is the default public user id i.e. the first one contained in P-Associated-URI;
AssociatedTelUri is the same as used in P-Associated-URI
PublicUserId2 and PublicUserId3 are the remaining IMPUs of the P-Associated-URI header

200 OK for NOTIFY (Step 3)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

8.15.5 Test requirements

UE shall not deregister from IMS between steps 1 and 2.

In step 4 (referring to the messages defined in annex C.2) all the requests sent by the UE contain the new updated home domain name and/or IMS identities which the UE has read from ISIM after step 1.

More specifically the UE shall use the new values read from ISIM for constructing the following headers:

Request-URI: HomeDomainName, IMPU
From: IMPU
To: IMPU
Authorization: PrivateUserIdentity, HomeDomainName

9 Authentication

9.1 Invalid Behaviour – MAC Parameter Invalid

9.1.1 Definition

To test that the UE when receiving an invalid 401 (Unauthorized) response to its initial REGISTER request behaves correctly. This procedure is described in 3GPP TS 24.229 [10] clause 5.1.1.5. The test case is applicable for IMS security.

9.1.2 Conformance requirement

When the network requires authentication or re-authentication of the UE, the UE will receive a 401 (Unauthorized) response to the REGISTER request.

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

1) extract the RAND and AUTN parameters;

2) check the validity of a received authentication challenge, as described in 3GPP TS 33.203 [19] i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

…

If, in a 401 (Unauthorized) response, either the MAC or SQN is incorrect the UE shall respond with a further REGISTER indicating to the S-CSCF that the challenge has been deemed invalid as follows:

- in the case where the UE deems the MAC parameter to be invalid the subsequent REGISTER request shall contain no "auts' Authorization header field parameter and an empty "response" Authorization header field parameter , i.e. no authentication challenge response;

- in the case where the UE deems the SQN to be out of range, the subsequent REGISTER request shall contain the "auts" Authorization header field parameter (see 3GPP TS 33.102[18]).

NOTE: In the case of the SQN being out of range, a "response" Authorization header field parameter can be included by the UE, based on the procedures described in RFC 3310 [49].

Whenever the UE detects any of the above cases, the UE shall:

- send the REGISTER request using an existing set of security associations, if available (see 3GPP TS 33.203 [19]);

- populate a new Security-Client header field within the REGISTER request and associated contact address, set to specify the security mechanism it supports, the IPsec layer algorithms for integrity and confidentiality protection it supports and the parameters needed for the new security association setup; and

- not create a temporary set of security associations.

On receiving a 420 (Bad Extension) response in which the Unsupported header field contains the value "sec-agree" and if the UE supports GPRS-IMS-Bundled authentication, the UE shall initiate a new authentication attempt with the GPRS-IMS-Bundled authentication procedures as specified in subclause 5.1.1.2.6.

Reference(s)

3GPP TS 24.229[10], clause 5.1.1.5.

9.1.3 Test purpose

1) To verify that after receiving a 401 (Unauthorized) response from S-CSCF for the initial REGISTER sent, the UE checks the validity of the received authentication challenge, as described in 3GPP TS 33.203 [14] i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge

2) If, the value of MAC derived from the AUTN part of the 401 (Unauthorized) received by the UE does not match the value of locally calculated XMAC:

   - the UE responds with a further REGISTER indicating to the S-CSCF that the challenge has been deemed invalid and:

   - this subsequent REGISTER request contains no "auts' Authorization header field parameter and an empty "response" Authorization header field parameter , i.e. no authentication challenge response

   - populates a new Security-Client header field within the REGISTER request and associated contact address, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the new security association setup; and

   - does not create a temporary set of security associations.

9.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services, but has an active PDP context and has discovered the SS as P-CSCF by executing the generic test procedure in Annex C.2 up to step 3.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17]. SS is listening to SIP default port 5060 for both UDP and TCP protocols.

Related ICS/IXIT Statement(s)

<To be added>

IMS security (Yes/No)

Test procedure

1) IMS registration is initiated on the UE. SS waits for the UE to send an initial REGISTER request, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.2

2) SS responds to the initial REGISTER request with an invalid 401 Unauthorized response, headers populated as follows:

   a) To, From, Via, CSeq, Call-ID and Content-Length headers according to RFC 3261 [15] clauses 8.2.6.2 and 20.14; and

   b) WWW-Authentication header with AKAv1-MD5 authentication challenge according to in 3GPP TS 24.229 [10], clause 5.4.1.2.1 and RFC 3310 [17] clause 3; except that the MAC value in AUTN should be incorrect and the CK and IK values are not included

   c) Security-Server header according to 3GPP TS 24.229 [10], clause 5.2.2 and RFC 3329 [21] clause 2.

3) SS waits for the UE to send a second Registration message indicating that the received 401 (Unauthorized) message was invalid

4) SS sends an invalid 401 (UNAUTHORIZED) message, same as in step b)

5) SS waits for the UE to send a second Registration message indicating that the received 401 (Unauthorized) message was invalid

NOTE: From this point onward the SS shall ignore any Registration message sent by the UE.

6) SS sends a 403 (Forbidden) message to the UE (to get the UE in a stable state at the end of the test case).

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE sends initial registration for IMS services.
2	←		401 Unauthorized	The SS responds with an invalid AKAv1-MD5 authentication challenge with an invalid MAC value.
3	→		REGISTER	REGISTER request: - contains no AUTS directive and an empty response directive, i.e. no authentication challenge response - UE populates a new Security-Client header set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the new security association setup
4	←		401 Unauthorized	The SS responds with an invalid AKAv1-MD5 authentication challenge with an invalid MAC value.
5	→		REGISTER	REGISTER request: - contains no AUTS directive and an empty response directive, i.e. no authentication challenge response - UE populates a new Security-Client header set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the new security association setup
				Note: From this point onward the SS shall ignore any Registration message sent by the UE.
6	←		403 Forbidden	The SS sends this message to get the UE in a stable state.

Specific message contents

401 UNAUTHORIZED (Steps 2 and 4)

Use the default message '401 Unauthorized for REGISTER' in annex A.1.2 with the following exceptions:

Header/param	Value/remark
WWW-Authenticate	
nonce	Base 64 encoding of RAND and AUTN, incorrect MAC value is used to generate

REGISTER (Step 1)

Use the default message 'REGISTER' in annex A.1.1 with condition A1

REGISTER (Steps 3 and 5)

Use the default message 'REGISTER' in annex A.1.1 with condition A1 with the following exceptions:

Header/param	Value/remark
CSeq	
value	The value sent in the previous REGISTER message + 1 (incremented)
Call-ID	
callid	The same value as in REGISTER in Step 1
Security-Verify	Header must not appear in the request
Authorization	
response	It shall be present but empty
auth-param	If present it shall not contain the auts='<base 64 encoded value>' directive
nonce-count	value or presence of the parameter not to be checked

403 FORBIDDEN (Step 6)

Use the default message '403 FORBIDDEN' in annex A.3.2.

9.1.5 Test requirements

SS shall check in step 3 and 5 that in accordance to the 3GPP TS 24.229 [10] clause 5.1.1.5

- the UE responds with a further REGISTER indicating to the S-CSCF that the challenge has been deemed invalid and:
- sends the REGISTER request using no security associations; and
- the REGISTER request contains no AUTS directive and an empty response directive, i.e. no authentication challenge; and
- populates a new Security-Client header within the REGISTER request, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the new security association setup; and
- does not create a temporary set of security associations.

9.2 Invalid Behaviour – SQN out of range

9.2.1 Definition

To test that the UE when receiving an invalid 401 (Unauthorized) response to its initial REGISTER request behaves correctly. This procedure is described in 3GPP TS 24.229 [10] clause 5.1.1.5. The test case is applicable for IMS security.

To test after a failed authentication attempt that the UE when receiving a valid 401 (Unauthorized) response to its initial REGISTER request behaves correctly. This procedure is described in 24.229 [10] clause 5.1.1.5.

9.2.2 Conformance requirement

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

1) extract the RAND and AUTN parameters;
2) check the validity of a received authentication challenge, as described in 3GPP TS 33.203 [19] i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

…

If, in a 401 (Unauthorized) response, either the MAC or SQN is incorrect the UE shall respond with a further REGISTER indicating to the S-CSCF that the challenge has been deemed invalid as follows:

- in the case where the UE deems the MAC parameter to be invalid the subsequent REGISTER request shall contain no "auts' Authorization header field parameter and an empty "response" Authorization header field parameter , i.e. no authentication challenge response;

- in the case where the UE deems the SQN to be out of range, the subsequent REGISTER request shall contain the "auts" Authorization header field parameter (see 3GPP TS 33.102[18]).

NOTE: In the case of the SQN being out of range, a "response" Authorization header field parameter can be included by the UE, based on the procedures described in RFC 3310 [49].

Whenever the UE detects any of the above cases, the UE shall:

- send the REGISTER request using an existing set of security associations, if available (see 3GPP TS 33.203[19]);

- populate a new Security-Client header field within the REGISTER request and associated contact address, set to specify the security mechanism it supports, the IPsec layer algorithms for integrity and confidentiality protection it supports and the parameters needed for the new security association setup; and

- not create a temporary set of security associations.

On receiving a 420 (Bad Extension) in which the Unsupported header field contains the value "sec-agree" and if the UE supports GPRS-IMS-Bundled authentication, the UE shall initiate a new authentication attempt with the GPRS-IMS-Bundled authentication procedures as specified in subclause 5.1.1.2.6.

Reference(s)

3GPP TS 24.229[10], clause 5.1.1.5.

9.2.3 Test purpose

1) To verify that after receiving a 401 (Unauthorized) response for the initial REGISTER sent, the UE checks that the SQN parameter derived from the AUTN part of the authentication challenge is within the correct range

2) If, the value of SQN derived from the AUTN part of the 401 (Unauthorized) received by the UE is out of range the UE reacts correctly:

3) To verify after a failed authentication attempt if the UE receives a valid 401 (Unauthorized) message from the network in response to the Register request sent, the UE is able to perform the authentication and registration successfully:

9.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services, but has an active PDP context and has discovered the SS as P-CSCF by executing the generic test procedure in Annex C.2 up to step 3.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17]. SS is listening to SIP default port 5060 for both UDP and TCP protocols.

Related ICS/IXIT Statement(s)

<To be added>

IMS security (Yes/No)

Test procedure

1) IMS registration is initiated on the UE. SS waits for the UE to send an initial REGISTER request, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.2

2) SS responds to the initial REGISTER request with an invalid 401 Unauthorized response, headers populated as follows:

   a) To, From, Via, CSeq, Call-ID and Content-Length headers according to RFC 3261 [15] clauses 8.2.6.2 and 20.14; and

   b) WWW-Authentication header with AKAv1-MD5 authentication challenge according to in 3GPP TS 24.229 [10], clause 5.4.1.2.1 and RFC 3310 [17] clause 3; except that the SQN value in AUTN should be out of range and the CK and IK values are not included

   c) Security-Server header according to 3GPP TS 24.229 [10], clause 5.2.2 and RFC 3329 [21] clause 2.

3) SS waits for the UE to send a second Registration message indicating that the received 401 (Unauthorized) message was invalid

4) SS sends a valid 401 (Unauthorized) message to the UE

5) SS waits for the UE to send a Registration request using the temporary set of security associations to protect the message. The Registration request shall contain the valid answer to the authentication challenge in 401 (Unauthorized) sent in the previous step

6) Continue test execution with the Generic test procedure in Annex C.2, step 7, sent over the same temporary set of security associations that the UE used for sending the REGISTER request

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE sends initial registration for IMS services.
2	←		401 Unauthorized	The SS responds with an invalid AKAv1-MD5 authentication challenge with SQN out of range.
3	→		REGISTER	REGISTER request: - contains AUTS directive - UE populates a new Security-Client header set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the new security association setup.
4	←		401 Unauthorized	This is a valid 401 (Unauthorized) message.
5	→		REGISTER	Message is sent using the temporary set of security associations to protect the message Contains the valid answer to the authentication challenge sent in the 401 (Unauthorized) message.
6	←→		Continue with Annex C.2 step 7	Execute the Generic test procedure Annex C.2 steps 7-11 in order to get the UE in a stable registered state.

Specific message contents

REGISTER (Step 1)

Use the default message 'REGISTER' in annex A.1.1 with condition A1.

401 UNAUTHORIZED (Step 2)

Use the default message '401 Unauthorized for REGISTER' in annex A.1.2 with the following exceptions:

Header/param	Value/remark
WWW-Authenticate	
nonce	Base 64 encoding of RAND and AUTN, Generated with SQN out of range with the AMF information field set to $AMF_{RESYNCH}$ value to trigger SQN re-synchronisation procedure in test USIM, see TS 34.108 clause 8.1.2.2.

REGISTER (Step 3)

Use the default message 'REGISTER' in annex A.1.1 with condition A1 with the following exceptions:

Header/param	Value/remark
CSeq	
value	The value sent in the previous REGISTER message + 1 (incremented)
Call-ID	
callid	The same value as in REGISTER in Step 1
Authorization	
nonce	Same value as the opaque value in the previous 401 UNAUTHORIZED message
opaque	Same value as the opaque value in the previous 401 UNAUTHORIZED message
response	parameter must exist, but value not to be checked
auth-param	auts= LDQUOT auts-value RDQUOT, auts-value not to be checked
nonce-count	value or presence of the parameter not to be checked

REGISTER (Step 5)

Use the default message 'REGISTER' in annex A.1.1 with condition A2.

9.2.5 Test requirements

SS shall check in step 3 that in accordance to the 3GPP TS 24.229 [10] clause 5.1.1.5

- the UE responds with a further REGISTER indicating to the S-CSCF that the challenge has been deemed invalid and:
- sends the REGISTER request using no security associations; and
- the REGISTER request contains "auts' Authorization header field parameter ; and
- populates a new Security-Client header within the REGISTER request, set to specify the security mechanism it supports, the IPsec layer algorithms it supports and the parameters needed for the new security association setup; and
- does not create a temporary set of security associations.

SS shall check in step 5 that in accordance to the 3GPP TS 24.229 [10] clause 5.1.1.5

- the UE sets up the temporary set of security associations between the ports announced in Security-Client header (UE) in the REGISTER request and Security-Server header (SS) in the 401 Unauthorized response;
- Sends the Registration request using the temporary set of security associations to protect the message

10 Subscription

10.1 Invalid Behaviour – 503 Service Unavailable

10.1.1 Definition and applicability

Test to verify that when the UE receives a 503 (Service Unavailable) response to a SUBSCRIBE request containing a Retry-After header, then the UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents. This can happen when the server is temporarily unable to process the request due to a temporary overloading or maintenance of the server. The test case is applicable for IMS security orGIBA.

10.1.2 Conformance requirement

[TS 24.229, clause 5.1.2.2]

If the UA receives a 503 (Service Unavailable) response to an initial SUBSCRIBE request containing a Retry-After header, then the UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents.

Reference(s)

3GPP TS 24.229[10], clause 5.1.2.2.

10.1.3 Test purpose

To verify that after receiving a 503 (Service Unavailable) response to a SUBSCRIBE request, containing a Retry-After header, the UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents. This can happen when the server is temporarily unable to process the request due to a temporary overloading or maintenance of the server.

10.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to step 7 or C.2a (GIBA only) up to step 5.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

GIBA (Yes/No)Test procedure

1) The UE sends a SUBSCRIBE request over the established security associations.

2) The SS responds to the SUBSCRIBE request with a 503 (Service Unavailable) response with the Retry-After header with period set to T, indicating how long the service is expected to be unavailable to the requesting client.

3) The SS waits for the period of time T defined in the Retry-After header, to check that the UE does not try to SUBSCRIBE for the registration event during this period.

4) The UE sends a new SUBSCRIBE request.

5) Continue test execution with the Generic test procedure in Annex C.2 or C.2a (GIBA only), step 9.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		SUBSCRIBE	UE subscribes to its registration event package.
2	←		503 Service Unavailable	The SS responds with 503 response containing a Retry-After header with period set to T.
3				SS waits for Time T to check that the UE does not re-attempt the request .
4	→		SUBSCRIBE	UE reattempts to subscribe to its registration event package.
5	←→		Continue with Annex C.2 step 9	Execute the Generic test procedure Annex C.2 steps 9-11 in order to get the UE in a stable registered state.

NOTE: The default messages contents in annex A are used with condition 'IMS security ' or 'GIBA' when applicable

Specific Message Contents

SUBSCRIBE (Step 1)

Use the default message 'SUBSCRIBE for reg-event package' in annex A.1.4 .

503 Service Unavailable response (Step 2)

Use the default message '503 Service Unavailable' in annex A.4.2.

SUBSCRIBE (Step 4)

Use the default message 'SUBSCRIBE for reg-event package' in annex A.1.4 with the following exception:

Header/param	Value/remark
Call-ID	
callid	value different from the previous SUBSCRIBE request

10.1.5 Test requirements

Step 3: The UE shall not automatically reattempt the request during the period duration T.

Step 4: The UE reattempts to send a SUBSCRIBE request for registration event package.

11 Notification

11.1 Network-initiated deregistration

11.1.1 Definition and applicability

Test to verify that the UE can correctly process the network initiated deregistration request. The test case is applicable for IMS security or early IMS security.

11.1.2 Conformance requirement

Upon receipt of a NOTIFY request on the dialog which was generated during subscription to the reg event package as described in subclause 5.1.1.3, including one or more <registration> element(s) which were registered by this UE with:

- the state attribute set to "terminated" and the event attribute within the <contact> element belonging to this UE set to "rejected" or "deactivated"; or

- the state attribute set to "active" and the state attribute within the <contact> element belonging to this UE set to "terminated", and associated event attribute element to "rejected" or "deactivated";

the UE shall remove all registration details relating to these public user identities. In case of a "deactivated" event attribute, the UE shall start the initial registration procedure as described in subclause 5.1.1.2. In case of a "rejected" event attribute, the UE shall release all dialogs related to those public user identities.

Upon receipt of a NOTIFY request, the UE shall delete the security associations towards the P-CSCF either:

- if all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header contains the value of "terminated"; or

- if each <registration> element that was registered by this UE has either the state attribute set to "terminated", or the state attribute set to "active" and the state attribute within the <contact> element belonging to this UE set to "terminated".

The UE shall delete these security associations towards the P-CSCF after the server transaction (as defined in RFC 3261 [26]) pertaining to the received NOTIFY request terminates.

NOTE 1: Deleting a security association is an internal procedure of the UE and does not involve any SIP procedures.

NOTE 2: If the security association towards the P-CSCF is removed, then the UE considers the subscription to the reg event package terminated (i.e. as if the UE had sent a SUBSCRIBE request with an Expires header containing a value of zero, or a NOTIFY request was received with Subscription-State header containing the value of "terminated").

Early IMS security:

NOTE 1: Early IMS security does not allow SIP requests to be protected using an IPsec security association because it does not perform a key agreement procedure

Reference(s)

3GPP TS 24.229[10], clause 5.1.1.7, 3GPP TR 33.978[59], clause 6.2.3.1.

11.1.3 Test purpose

To verify that UE will not try registration after getting a NOTIFY with all <registration> element(s) set to "terminated" and "rejected".

11.1.4 Method of test

Initial conditions

UE contains either SIM application (early IMS security), ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (early IMS security only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

Early IMS security (Yes/No)

Test procedure

1) SS sends UE a NOTIFY request for the subscribed registration event package, indicating that registration for all the previously registered user identities has been terminated and that new registration shall not be performed. Request is sent over the existing security associations between SS and UE.

2) SS waits for the UE to respond the NOTIFY with 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		NOTIFY	The SS sends a NOTIFY for registration event package, containing full registration state information, with all previously registered public user identities "terminated" and "rejected"
2	→		200 OK	The UE responds the NOTIFY with 200 OK

NOTE: The default messages contents in annex A are used with condition 'IMS security ' or 'early IMS security' when applicable

Specific Message Contents

NOTIFY (Step 1)

Use the default message 'NOTIFY for reg-event package' in annex A.1.6 with the following exceptions:

Header/param	Value/remark
CSeq	
value	*2*
Subscription-State	
substate-value	*terminated*
expires	*0*
Message-body	<?xml version='1.0?> <reginfo xmlns='urn:ietf:params:xml:ns:reginfo' version='1' state='full'> <registration aor='PublicUserIdentity1 (NOTE 1)' id='a100' state='terminated'> <contact id='980' state='terminated' event='rejected'> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> <registration aor='AssociatedTelUri (NOTE 1)' id='a101' state='terminated'> <contact id='981' state='terminated' event='rejected'> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> <registration aor='PublicUserIdentity2 (NOTE 1)' id='a102' state='terminated'> <contact id='982' state='terminated' event='rejected'> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> <registration aor='PublicUserIdentity3 (NOTE 1)' id='a103' state='terminated'> <contact id='983' state='terminated' event='rejected'> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration></reginfo>

NOTE 1: The public user ids and the associated TEL URI are as returned to the UE in the P-Associated-URI header of the 200 (OK) response to the REGISTER request;
PublicUserId1 is the default public user id i.e. the first one contained in P-Associated-URI;
AssociatedTelUri is the same as used in P-Associated-URI
PublicUserId2 and PublicUserId3 are the remaining IMPUs of the P-Associated-URI header

200 OK for NOTIFY (Step 2)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

11.1.5 Test requirements

Step 2: SS shall check that the UE sends the 200 OK response over the existing set of security associations.

SS shall check that terminal does not try to send a REGISTER message after sending 200 OK. Waiting period of one minute is sufficient.

11.2 Network initiated re-authentication

11.2.1 Definition and applicability

Test to verify that the UE can correctly process the network initiated re-authentication request and re-authenticate the user before the registration expires, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.2. The test case is applicable for IMS security.

11.2.2 Conformance requirement

At any time, the UE can receive a NOTIFY request carrying information related to the reg event package (as described in subclause 5.1.1.3). If:

- the state attribute in any of the <registration> elements is set to "active";
- the value of the <uri> sub-element inside the <contact> sub-element is set to the Contact address that the UE registered; and
- the event attribute of that <contact> sub-element(s) is set to "shortened";

the UE shall:

1) use the expiry attribute within the <contact> sub-element that the UE registered to adjust the expiration time for that public user identity; and
2) start the re-authentication procedures at the appropriate time (as a result of the S-CSCF procedure described in subclause 5.4.1.6) by initiating a reregistration as described in subclause 5.1.1.4, if required.

NOTE: When authenticating a given private user identity, the S-CSCF will only shorten the expiry time within the <contact> sub-element that the UE registered using its private user identity. The <contact> elements for the same public user identity, if registered by another UE using different private user identities remain unchanged. The UE will not initiate a reregistration procedure, if none of its <contact> sub-elements was modified.

Reference(s)

3GPP TS 24.229[10], clause 5.1.1.5.2.

11.2.3 Test purpose

1) To verify that UE adjusts the expiration time for a public user identity as indicated within the received NOTIFY related to reg event package; and

2) To verify that the UE will start the re-authentication procedures at the appropriate time before the registration expires.

11.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services by executing the generic test procedure in Annex C.2 up to the last step.. The expiration time for the registration must be at least 600 seconds. Security associations have been set up between UE and the SS.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

Test procedure

1) SS sends UE a NOTIFY request for the subscribed registration event package, indicating the shortened expiration time as 60 seconds. Request is sent over the existing security associations between SS and UE.

2) SS waits for the UE to respond the NOTIFY with 200 OK response.

3) SS waits for the UE send a REGISTER request 30 seconds before the expected new expiration time.

4) SS responds to the REGISTER request with a valid 401 Unauthorized response, headers populated according to the 401 response common message definition.

5) SS waits for the UE to set up a new set of security associations and send another REGISTER request, over those security associations.

6) The SS responds with 200 OK over the new security association

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		NOTIFY	The SS sends a NOTIFY for registration event package, containing partial registration state information, indicating shortened expiration time (60 seconds) for the registered public user identity in the XML body.
2	→		200 OK	The UE responds the NOTIFY with 200 OK.
3	→		REGISTER	UE re-registers the user 30 seconds before the expected expiration.
4	←		401 Unauthorized	The SS responds with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network.
5	→		REGISTER	UE completes the security negotiation procedures, sets up a new temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials.
6	<-		200 OK	The UE responds with 200 OK.

Specific Message Contents

NOTIFY (Step 1)

Use the default message 'NOTIFY for reg-event package' in annex A.1.6 with the following exceptions:

Header/param	Value/remark
CSeq	
value	2
Message-body	*<?xml version='1.0?>* *<reginfo xmlns='urn:ietf:params:xml:ns:reginfo' version='1' state='partial'>* *<registration aor=*'any IMPU within the set of IMPUs on ISIM' *id='a100' state='active'>* *<contact id='980' state='active' event='shortened' expires="60">* <*uri*>same value as in Contact header of REGISTER request*</uri>* *</contact>* *</registration>* *</reginfo>*

200 OK for NOTIFY (Step 2)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

REGISTER (Step 3)

Use the default message 'REGISTER' in annex A.1.1 condition A2 with the following exceptions:

Header/param	Value/remark
Security-Client	
spi-c	new SPI number of the inbound SA at the protected client port
spi-s	new SPI number of the inbound SA at the protected server port
port-c	new protected client port needed for the setup of new pairs of security associations
port-s	Same value as in the previous REGISTER

401 Unauthorized for REGISTER (Step 4)

Use the default message '401 Unauthorized for REGISTER' in annex A.1.2 with the following exceptions:

Header/param	Value/remark
Security-Server	
spi-c	new SPI number of the inbound SA at the protected client port
spi-s	new SPI number of the inbound SA at the protected server port
port-c	new protected client port needed for the setup of new pairs of security associations
port-s	Same value as in the previous Security-Server headers
WWW-Authenticate	
nonce	Base 64 encoding of a new RAND and AUTN

REGISTER (Step 5)

Use the default message 'REGISTER' in annex A.1.1 with condition A2.

11.2.5 Test requirements

Step 2: SS shall check that the UE sends the 200 OK response over the existing set of security associations.

Step 3: SS shall check that in accordance to the 3GPP TS 24.229 [10] clause 5.1.1.4 the UE sends a REGISTER request over the existing set of security associations.

12 Call Control

12.1 Void

12.2 MO Call – 503 Service Unavailable

12.2.1 Definition

When a server is temporarily unable to process an INVITE request due to a temporary overloading or maintenance of the server sends a 503 Service Unavailable response. The server may indicate when the service will be available again in a Retry-After header field. This process is described in 3GPP TS 24.229 [10], clause 5.1.3.1. The test case is applicable for IMS security orGIBA.

12.2.2 Conformance requirement

Upon receiving a 503 (Service Unavailable) response to an initial INVITE request containing a Retry-After header, then the originating UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents.

Reference(s)

3GPP TS 24.229[10], clause 5.1.3.1.

12.2.3 Test purpose

To verify that when the UE receives a 503 (Service Unavailable) response to an initial INVITE request containing a Retry-After header, then the UE shall not automatically reattempt the request until after the period indicated by the Retry-After header contents.

12.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for IMS Multimedia Telephony (Yes/No)

Support for speech (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

For value of T see specific message content for 503 (Service Unavailable) message.

1-8) UE executes the procedures described in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 8.

9) The SS responds with a 503 (Service Unavailable) response with the Retry-After header set to T.

10) The SS waits for the UE to send an ACK to acknowledge the reception of the 503 (Service Unavailable) response.

11) SS waits for a duration of time T and checks that the UE does not reattempt sending the INVITE request. After the time T the UE may reattempt sending the INVITE request.

12) The UE may reattempt sending the INVITE request after time T.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-3			Steps defined in annex C.21	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.6.3-1 for a UE with E-UTRA support.
4	←		503 Service Unavailable	Including Retry-After header with period set to T
5	→		ACK	The UE acknowledges the reception of the 503 (Service Unavailable) response
6				The SS waits for a duration of time T and checks that the UE does not re-send the INVITE request
7			Step 1 defined in annex C.21	Optional

NOTE: The default messages contents in annex A are used with condition 'IMS security' or 'GIBA' when applicable

Specific Message Contents

Steps 1 - 3 as specified in annex C.21

503 Service Unavailable (Step 4)

Use the default message '503 Service Unavailable' in annex A.4.2.

ACK (Step 5)

Use the default message 'ACK' in annex A.2.7 with the following exceptions:

Header/param	Value/remark
route	As in the intial INVITE request sent by the UE

12.2.5 Test requirements

At step 6 the UE shall not reattempt the INVITE request before time T from the time the SS receives the ACK from the UE in step 5.

12.2a MO Call – 504 Server Time-out

12.2a.1 Definition

When a the S-CSCFS server is temporarily unable to process an INVITE as the S-CSCF does not have the user profile or does not trust the data that it has (e.g. due to restart), the S-CSCF can rejects the request by returning a 504 (Server Time-out) response to the UE with specific content as specified in [1] clause 5.4.3.2. As a result the UE will initiate restoration procedures by performing an initial registration.

12.2a.2 Conformance requirement

In the event the UE receives a 504 (Server Time-out) response containing:

1) a P-Asserted-Identity header field set to a value equal to a URI:

   a) from the Service-Route header field value received during registration; or

   b) from the Path header field value received during registration; and

2) a Content-Type header field set according to subclause 7.6 (i.e. "application/3gpp-ims+xml"), independent of the value or presence of the Content-Disposition header field, independent of the value or presence of Content-Disposition parameters, then the default content disposition, identified as "3gpp-alternative-service", is applied as follows:

   a) if the 504 (Server Time-out) response includes an IM CN subsystem XML body as described in subclause 7.6 with the <ims-3gpp> element, including a version attribute, with the <alternative-service> child element:

      a) with the <type> child element set to "restoration" (see table 7.7AA); and

      b) with the <action> child element set to "initial-registration" (see table 7.7AB);

      then the UE:

      - shall initiate restoration procedures by performing an initial registration as specified in subclause 5.1.1.2; and

- may provide an indication to the user based on the text string contained in the <reason> child element of the <alternative-service> child element of the <ims-3gpp> element.

Reference(s)

3GPP TS 24.229[10], clause 5.1.2A.1.6,

12.2a.3 Test purpose

To verify that when the UE receives a 504 (Server Time-out) response to an INVITE request containing a P-Asserted-Identity header field set to a value equal to a URI from the Service-Route header field value received during registration and the rest of the message is set as described in [1] subclause 5.1.2A.1.6, then the UE initiates restoration procedures by performing an initial registration as specified in subclause 5.1.1.2.

12.2a.4 Method of test

Initial conditions

UE contains an ISIM and USIM or only USIM application on the UICC. UE has activated a PDP context/EPS bearer, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for IMS Multimedia Telephony (Yes/No)

Support for speech (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

IMS security (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-8) UE executes the procedures described in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 8.

9) The SS responds with a 504 (Server Time-out) response.

10) The SS waits for the UE to send an ACK to acknowledge the reception of 504 (Server Time-out) response.

11-18) As specified in steps 4-11 annex C.2.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-2			Steps defined in annex C.21	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.6.3-1 for a UE with E-UTRA support.
3	←		504 Server Time-out	Set as per the specific message contents
4	→		ACK	
5-12	→		Steps 4-11 annex C.2	The UE performs an initial registration

NOTE: The default messages contents in annex A are used with condition 'IMS security' or 'early IMS security' when applicable

Specific Message Contents

Steps 1-2

As specified in annex C.21

504 Server Time-out (Step 3)

Use the default message '504 Server Time-out' in annex A.4. 6

ACK (Step 4)

As specified in annex A.2.7.

Steps 5-12

As specified in annex C.2.

12.2a.5 Test requirements

After step 3 the UE shall perform an initial registration.

12.3 to 12.11 Void

12.12 MO MTSI Voice Call Successful with preconditions

12.12.1 Definition and applicability

Test to verify that the UE correctly performs IMS mobile originated voice call setup and release when using IMS Multimedia Telephony with preconditions. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1, TS 24.173 [65] and TS 26.114 [66]. The test case is applicable for IMS security or GIBA.

12.12.2 Conformance requirement

[TS 24.229, clause 5.1.2A.1]:

The procedures of this subclause are general to all requests and responses, except those for the REGISTER method.

When the UE sends any request using a given contact address, the UE shall:

- if IMS AKA is in use as a security mechanism:

  a) if the UE has not obtained a GRUU, populate the Contact header field of the request with the protected server port and the respective contact address; and

  b) include the protected server port and the respective contact address in the Via header field entry relating to the UE;

...

- if GPRS-IMS-Bundled authentication is in use as a security mechanism, and therefore no port is provided for subsequent SIP messages by the P-CSCF during registration, the UE shall send any request to the same port used for the initial registration as described in subclause 5.1.1.2.

...

The UE shall determine the public user identity to be used for this request as follows:

1) if a P-Preferred-Identity was included, then use that as the public user identity for this request; or

2) if no P-Preferred-Identity was included, then use the default public user identity for the security association or TLS session and the associated contact address as the public user identity for this request;

The UE shall not include its "+sip.instance" header field parameter in the Contact header field in its non-register requests and responses except when the request or response is guaranteed to be sent to a trusted intermediary that will remove the "+sip.instance" header field parameter prior to forwarding the request or response to the destination.

NOTE 6: Such trusted intermediaries include an AS that all such requests as part of an application or service traverse. In order to ensure that all requests or responses containing the "+sip.instance" header field parameter are forwarded via the trusted intermediary the UE needs to have first verified that the trusted intermediary is present (e.g. first contacted via a registration or configuration procedure).

If this is a request for a new dialog, the Contact header field is populated as follows:

1) a contact header value which is one of:

   - if a public GRUU value ("pub-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does not indicate privacy of the P-Asserted-Identity, then the UE should insert the public GRUU ("pub-gruu" header field parameter) value as specified in RFC 5627; or

   - if a temporary GRUU value ("temp-gruu" header field parameter) has been saved associated with the public user identity to be used for this request, and the UE does indicate privacy of the P-Asserted-Identity, then the UE should insert the temporary GRUU ("temp-gruu" header field parameter) value as specified in RFC 5627; or

- otherwise, a SIP URI containing the contact address of the UE;

NOTE 7: The above items are mutually exclusive.

2) include an "ob" SIP URI parameter, if the UE supports multiple registrations, and the UE wants all subsequent requests in the dialog to arrive over the same flow identified by the flow token as described in RFC 5626;

3) if the request is related to an IMS communication service that requires the use of an ICSI then the UE shall include in a g.3gpp.icsi-ref media feature tag, as defined in subclause 7.9.2 and RFC 3841, the ICSI value (coded as specified in subclause 7.2A.8.2) for the IMS communication service. The UE may also include other ICSI values that the UE is prepared to use for all dialogs with the terminating UE(s); and

4) if the request is related to an IMS application that is supported by the UE, then the UE may include in a g.3gpp.iari-ref media feature tag, as defined in subclause 7.9.3 and RFC 3841, the IARI value (coded as specified in subclause 7.2A.9.2) that is related to the IMS application and that applies for the dialog.

...

If this is a request for a new dialog or standalone transaction and the request is related to an IMS communication service that requires the use of an ICSI then the UE:

1) shall include the ICSI value (coded as specified in subclause 7.2A.8.2), for the IMS communication service that is related to the request in a P-Preferred-Service header field according to draft-drage-sipping-service-identification. If a list of network supported ICSI values was received as specified in 3GPP TS 24.167, the UE shall only include an ICSI value that is in the received list;

NOTE 8: The UE only receives those ICSI values corresponding to the IMS communication services that the network provides to the user.

2) may include an Accept-Contact header field containing an ICSI value (coded as specified in subclause 7.2A.8.2) that is related to the request in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 if the ICSI for the IMS communication service is known.

NOTE 9: If the UE includes the same ICSI values into the Accept-Contact header field and the P-Preferred-Service header field, there is a possibility that one of the involved S-CSCFs or an AS changes the ICSI value in the P-Asserted-Service header field, which results in the message including two different ICSI values (one in the P-Asserted-Service header field, changed in the network and one in the Accept-Contact header field).

If an IMS application indicates that an IARI is to be included in a request for a new dialog or standalone transaction, the UE shall include an Accept-Contact header field containing an IARI value (coded as specified in subclause 7.2A.9.2) that is related to the request in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3841.

NOTE 10: RFC 3841 allows multiple Accept-Contact header fields along with multiple Reject-Contact header fields in a SIP request, and within those header fields, expressions that include one or more logical operations based on combinations of media feature tags. Which registered UE will be contacted depends on the Accept-Contact header field and Reject-Contact header field combinations included that evaluate to a logical expression and the relative qvalues of the registered contacts for the targeted registered public user identity. There is therefore no guarantee that when multiple Accept-Contact header fields or additional Reject-Contact header field(s) along with the Accept-Contact header field containing the ICSI value or IARI value are included in a request that the request will be routed to a contact that registered the same ICSI value or IARI value. Charging and accounting is based upon the contents of the P-Asserted-Service header field and the actual media related contents of the SIP request and not the Accept-Contact header field contents or the contact reached.

NOTE 11: The UE only includes the header field parameters "require" and "explicit" in the Accept-Contact header field containing the ICSI value or IARI value if the IMS communication service absolutely requires that the terminating UE understand the IMS communication service in order to be able to accept the session. Including the header field parameters "require" and "explicit" in Accept-Contact header fields in requests which don"t absolutely require that the terminating UE understand the IMS communication service in order to accept the session creates an interoperability problem for sessions which otherwise would interoperate and violates the interoperability requirements for the ICSI in 3GPP TS 23.228.

...

If available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall insert a P-Access-Network-Info header field into any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method (see subclause 7.2A.4).

NOTE 13: During the dialog, the points of attachment to the IP-CAN of the UE may change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header field in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header field value for all new dialogs and standalone transactions. The UE shall build a list of Route header field values made out of the following, in this order:

a) the P-CSCF URI containing the IP address or the FQDN learnt through the P-CSCF discovery procedures; and

b) the P-CSCF port based on the security mechanism in use:

- if IMS AKA or SIP digest with TLS is in use as a security mechanism, the protected server port learnt during the registration procedure;

- if SIP digest without TLS, NASS-IMS bundled authentication or GPRS-IMS-Bundled authentication is in use as a security mechanism, the unprotected server port used during the registration procedure;

c) and the values received in the Service-Route header field saved from the 200 (OK) response to the last registration or re-registration of the public user identity with associated contact address.

[TS 24.229, clause 5.1.2A.1.2]:

The UE may use non-international formats of E.164 addresses, including geo-local numbers and home-local numbers and other local numbers (e.g. private number), in the Request-URI.

Local numbering information is sent in the Request-URI in initials requests or stand alone transaction, using one of the following formats:

1) a tel-URI, complying with RFC 3966, with a local number followed by a "phone-context" tel URI parameter value.

2) a SIP URI, complying with RFC 3261, with the "user" SIP URI parameter set to "phone"

3) a SIP URI, complying with RFC 3261 and RFC 4967, with the "user" SIP URI parameter set to "dialstring"

The actual value of the URI depends on whether user equipment performs an analysis of the dial string input by the end user or not.

[TS 24.229, clause 5.1.2A.1.5]:

When the UE uses home-local number, the UE shall include in the "phone-context" tel URI parameter the home domain name in accordance with RFC 3966.

When the UE uses geo-local number, the UE shall:

- if access technology information available to the UE (i.e., the UE can insert P-Access-Network-Info header field into the request), include the access technology information in the "phone-context" tel URI parameter according to RFC 3966 as defined in subclause 7.2A.10; and

- if access technology information is not available to the UE (i.e., the UE cannot insert P-Access-Network-Info header field into the request), include in the "phone-context" tel URI parameter the home domain name prefixed by the "geo-local." string according to RFC 3966 as defined in subclause 7.2A.10.

When the UE uses other local numbers, than geo-local number or home local numbers , e.g. private numbers that are different from home-local number, the UE shall include a "phone-context" tel URI parameter set according to RFC 3966, e.g. if private numbers are used a domain name to which the private addressing plan is associated.

NOTE 1: The "phone-context" tel URI parameter value can be entered or selected by the subscriber, or can be a "pre-configured" value inserted by the UE, based on implementation.

NOTE 2: The way how the UE determines whether numbers in a non-international format are geo-local, home-local or relating to another network, is implementation specific.

NOTE 3: Home operator's local policy can define a prefix string(s) to enable subscribers to differentiate dialling a geo-local number and/or a home-local number.

[TS 24.229, clause 5.1.3.1]:

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 as updated by RFC 4032.

The precondition mechanism should be supported by the originating UE.

The UE may initiate a session without the precondition mechanism if the originating UE does not require local resource reservation.

NOTE 1: The originating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

In order to allow the peer entity to reserve its required resources, an originating UE supporting the precondition mechanism should make use of the precondition mechanism, even if it does not require local resource reservation.

Upon generating an initial INVITE request using the precondition mechanism, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism; and

- indicate the support for the preconditions mechanism and specify it using the Supported header mechanism.

Upon generating an initial INVITE request using the precondition mechanism, the UE should not indicate the requirement for the precondition mechanism by using the Require header mechanism.

NOTE 2: If an UE chooses to require the precondition mechanism, i.e. if it indicates the "precondition" option tag within the Require header, the interworking with a remote UE, that does not support the precondition mechanism, is not described in this specification.

NOTE 3: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261. The UE can accept or reject any of the forked responses, for example, if the UE is capable of supporting a limited number of simultaneous transactions or early dialogs.

Upon successful reservation of local resources the UE shall confirm the successful resource reservation (see subclause 6.1.2) within the next SIP request.

NOTE 4: In case of the precondition mechanism being used on both sides, this confirmation will be sent in either a PRACK request or an UPDATE request. In case of the precondition mechanism not being supported on one or both sides, alternatively a reINVITE request can be used for this confirmation, in case the terminating UE does not support the PRACK request (as described in RFC 3262) and does not support the UPDATE request (as described in RFC 3311).

....

When a final answer is received for one of the early dialogues, the UE proceeds to set up the SIP session. The UE shall not progress any remaining early dialogues to established dialogs. Therefore, upon the reception of a subsequent final 200 (OK) response for an INVITE request (e.g., due to forking), the UE shall:

1) acknowledge the response with an ACK request; and

2) send a BYE request to this dialog in order to terminate it.

[TS 24.229, clause 6.1.1]:

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 as updated by RFC 4032.

In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.

During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261.

...

For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor and the "AS" bandwidth modifier in the SDP.

...

If the media line in the SDP indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556, then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in subclause 6.1 of RFC 3890.

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in 3GPP TS 29.208.

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifier will typically get the value of zero.

The UE shall include the MIME subtype "telephone-event" in the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 4733.

The UE shall inspect the SDP contained in any SIP request or response, looking for possible indications of grouping of media streams according to RFC 3524 and perform the appropriate actions for IP-CAN bearer establishment for media according to IP-CAN specific procedures (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

If resource reservation is needed, the UE shall start reserving its local resources whenever it has sufficient information about the media streams, media authorization and used codecs available.

NOTE 2: Based on this resource reservation can, in certain cases, be initiated immediately after the sending or receiving of the initial SDP offer.

...

[TS 24.229, clause 6.1.2]:

An INVITE request generated by a UE shall contain a SDP offer and at least one media description. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session.

If the desired QoS resources for one or more media streams have not been reserved at the UE when constructing the SDP offer, the UE shall:

- indicate the related local preconditions for QoS as not met, using the segmented status type, as defined in RFC 3312 and RFC 4032, as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1); and,

- set the related media streams to inactive, by including an "a=inactive" line, according to the procedures described in RFC 4566, unless the UE knows that the precondition mechanism is supported by the remote UE.

NOTE 1: When setting the media streams to the inactive mode, the UE can include in the first SDP offer the proper values for the RS and RR modifiers and associate bandwidths to prevent the receiving of the RTCP packets, and not send any RTCP packets.

If the desired QoS resources for one or more media streams are available at the UE when the initial SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 and RFC 4032, as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1).

NOTE 2: If the originating UE does not support the precondition mechanism it will not include any precondition information in SDP.

...

Upon generating the SDP offer for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the UE shall include SDP payload containing a subset of the allowed media types, codecs and other parameters from the SDP payload of all 488 (Not Acceptable Here) responses related to the same session establishment attempt (i.e. a set of INVITE requests used for the same session establishment). The UE shall order the codecs in the SDP payload according to the order of the codecs in the SDP payload of the 488 (Not Acceptable Here) response.

NOTE 3: The UE can attempt a session establishment through multiple networks with different policies and potentially can need to send multiple INVITE requests and receive multiple 488 (Not Acceptable Here) responses from different CSCF nodes. The UE therefore takes into account the SDP contents of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE request.

Upon confirming successful local resource reservation, the UE shall create a SDP offer in which:

- the related local preconditions are set to met, using the segmented status type, as defined in RFC 3312 and RFC 4032; and

- the media streams previously set to inactive mode are set to active (sendrecv, sendonly or recvonly) mode.

Upon receiving an SDP answer, which includes more than one codec for one or more media streams, the UE shall send an SDP offer at the first possible time, selecting only one codec per media stream.

[TS 26.114, clause 5.2.1]

MTSI clients in terminals offering speech communication shall support:

- AMR speech codec (3GPP TS 26.071 , 3GPP TS 26.090, 3GPP TS 26.073 and 3GPP TS 26.104) including all 8 modes and source controlled rate operation 3GPP TS 26.093 . The MTSI client in terminal shall be capable of operating with any subset of these 8 codec modes.

[TS 26.114 Rel-8, clause 6.2.2.1]:

An MTSI client offering a speech media session for narrow-band speech and/or wide-band speech should offer SDP according to the examples in clauses A.1 to A.3.

An MTSI client shall at least offer AVP for speech media streams. An MTSI client should also offer AVPF for speech media streams. RTP profile negotiation shall be done as described in clause 6.2.1a. RTP profile negotiation shall be done as described in clause 6.2.1a.

[TS 26.114, clause 7.3.1]:

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556 . Therefore, an MTSIclient shall include the "b=RS:" and "b=RR:" fields in SDP, and shall be able to interpret them. There shall be an upper limit on the allowed RTCP bandwidth for each RTP session signalled by the MTSI client. This limit is defined as follows:

- 4 000 bps for the RS field (at media level);

- 3 000 bps for the RR field (at media level).

If the session described in the SDP is a point-to-point speech only session, the MTSI client may request the deactivation of RTCP by setting its RTCP bandwidth modifiers to zero.

GIBA:

NOTE 1: GIBA does not allow SIP requests to be protected using an IPsec security association because it does not perform a key agreement procedure.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.2A.1, 5.1.3 and 6.1, TR 33.978[59], clause 6.2.3.1., and TS 26.114 [66], clauses 5.2.1, 6.2.2.1 and 7.3.1.

12.12.3 Test purpose

1) To verify that when initiating MO call the UE performs correct exchange of SIP protocol signalling messages for setting up the session; and

2) To verify that within SIP signalling the UE performs the correct exchange of SDP messages for negotiating media and indicating preconditions for resource reservation (as described by 3GPP TS 24.229 [10], clause 6.1).

3) To verify that the UE is able to release the call.

12.12.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Related ICS/IXIT Statement(s)

- Support for initiating a session (Yes/No)
- Support for IMS Multimedia Telephony (Yes/No)
- Support for speech (Yes/No)
- Support for integration of resource management and SIP (use of preconditions) (Yes/No)
- IMS security (Yes/No)
- GIBA (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-14) UE executes the procedures described in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to14.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-13			Steps defined in annex C.21	MTSI MO speech call. Referred from 36.508 [94] table 4.5A.6.3-1 for a UE with E-UTRA support.
13A			The UE is triggered by MMI to release the call	
14	→		BYE	The UE releases the call with BYE
15	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

Steps 1 - 13 as specified in annex C.21

BYE (Step 14)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE (Step 15)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

12.12.5 Test requirements

SS must check that if the UE uses IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

Step 14: the UE shall send a BYE request with the correct content, according to common message definitions.

12.13 MT MTSI speech call

12.13.1 Definition and applicability

Test to verify that the UE correctly performs IMS mobile terminated speech call setup when using IMS Multimedia Telephony. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1, TS 24.173 [65] and TS 26.114 [66]. The test case is applicable for IMS security orGIBA.

12.13.2 Conformance requirement

[TS 24.229, clause 5.1.4.1]

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires local resource reservation.

NOTE 1: The terminating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

If local resource reservation is required at the terminating UE and the terminating UE supports the precondition mechanism, and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header or Require header, the terminating UE shall make use of the precondition mechanism and shall indicate a Require header with the "precondition" option-tag in any response or subsequent request it sends towards to the originating UE; or

…

If local resource reservation is not required by the terminating UE andthe terminating UE supports the precondition mechanism and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header and:

- the required resources at the originating UE are not reserved, the terminating UE shall use the precondition mechanism; or

[TS 24.229, clause 6.1.3]

If the terminating UE had previously set one or more media streams to inactive mode and the QoS resources for those media streams are now ready, it shall set the media streams to active mode by applying the procedures described in RFC 4566 with respect to setting the direction of media streams.

…

Upon sending a SDP answer to an SDP offer, with the SDP answer including one or more media streams for which the originating side did indicate its local preconditions as not met, if the precondition mechanism is supported by the terminating UE, the terminating UE shall indicate its local preconditions and request the confirmation for the result of the resource reservation at the originating end point.

[TS 26.114, clause 5.2.1]

MTSI terminals offering speech communication shall support:

- AMR speech codec (3GPP TS 26.071, 3GPP TS 26.090, 3GPP TS 26.073 and 3GPP TS 26.104) including all 8 modes and source controlled rate operation 3GPP TS 26.093. The terminal shall be capable of operating with any subset of these 8 codec modes.

[TS 26.114, clause 6.2.2.1]

An MTSI client offering a speech media session for narrow-band speech and/or wide-band speech should offer SDP according to the examples in clauses A.1 to A.3.

An MTSI client shall at least offer AVP for speech media streams. An MTSI client should also offer AVPF for speech media streams. RTP profile negotiation shall be done as described in clause 6.2.1a.

[TS 26.114, clause 6.2.5]

The SDP shall include bandwidth information for each media stream and also for the session in total. The bandwidth information for each media stream and for the session is defined by the Application Specific (AS) bandwidth modifier as defined in RFC 4566.

[TS 26.114, clause 7.3.1]

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556.

Reference(s)

3GPP TS 24.229[10] clauses 5.1.4.1, 6.1.3, TS 26.114 [66] clause 5.2.1, 6.2.2.1, 6.2.5 and 7.3.1.

12.13.3 Test purpose

1) To verify that, when initiating MT MTSI speech call and SS needs to reserve resources, the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

4) To verify that the UE is able to release the call.

12.13.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipp5ed into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

GIBA (Yes/No)

Support for initiating a session (Yes/No)

Support for speech (Yes/No)

Support for IMS Multimedia Telephony (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-26) UE executes the procedures described in TS 36.508 [94] table 4.5A.7.3-1 steps 1 to26.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-15			Steps defined in annex C.11	MTSI MT speech call. Referred from 36.508 [94] table 4.5A.7.3-1 for a UE with E-UTRA support.

NOTE: The default messages contents in annex A are used with condition 'IMS security' or 'GIBA' when applicable

Specific Message Content

None.

12.13.5 Test requirements

The UE shall send requests and responses as described in clause 12.13.4

12.14 Void

12.15 Void

12.16 MO MTSI Text call

12.16.1 Definition and applicability

Test to verify that the UE correctly performs mobile originated call setup and release for MTSI text call. The test case is applicable for IMS security orGIBA.

12.16.2 Conformance requirement

[TS 24.229, clause 5.1.3.1]

Upon generating an initial INVITE request using the precondition mechanism, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism;and
- indicate the support for the preconditions mechanism and specify it using the Supported header mechanism.

[TS 24.229, clause 6.1.2]

An INVITE request generated by a UE shall contain a SDP offer and at least one media description. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session.

…

If the desired QoS resources for one or more media streams are available at the UE when the SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 and RFC 4032, as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1).

[TS 26.114, clause 6.2.5]

The SDP shall include bandwidth information for each media stream and also for the session in total. The bandwidth information for each media stream and for the session is defined by the Application Specific (AS) bandwidth modifier as defined in RFC 4566.

[TS 26.114, clause 7.3.1]

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556.

The following RTP payload format shall be used:

- T.140 text conversation RTP payload format according to RFC 4103.

Real-time text shall be the only payload type in its RTP stream because the RTP sequence numbers are used for loss detection and recovery. The redundant transmission format shall be used for keeping the effect of packet loss low.

Reference(s)

3GPP TS 24.229[10] clauses 5.1.3.1, 6.1.2, TS 26.114[66] clause 6.2.5, 7.3.1 and 7.4.4.

12.16.3 Test purpose

1) To verify that when initiating MO MTSI text call the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

4) To verify that the UE is able to release the call.

12.16.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

Support for text (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Support for IMS Multimedia Telephony (Yes/No)

Test procedure

1) Execute annex C.15

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-8			Steps defined in annex C.15	MTSI MO text call

NOTE: The default messages contents in annex A are used with condition 'IMS security' or 'GIBA' when applicable

Specific Message Content

-

12.16.5 Test requirements

The UE shall send requests and responses as described in clause 12.16.4.

12.17 MT MTSI text call

12.17.1 Definition and applicability

Test to verify that the UE correctly performs IMS mobile terminated text call setup when using IMS Multimedia Telephony. This process is described in 3GPP TS 24.229 [10], clauses 5.1.4.1, TS 24.173 [65] and TS 26.114 [66]. The test case is applicable for IMS security orGIBA.

12.17.2 Conformance requirement

[TS 24.229, clause 5.1.4.1]

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires local resource reservation.

NOTE 1: The terminating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

If local resource reservation is required at the terminating UE and the terminating UE supports the precondition mechanism, and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header or Require header, the terminating UE shall make use of the precondition mechanism and shall indicate a Require header with the "precondition" option-tag in any response or subsequent request it sends towards to the originating UE; or

[TS 26.114, clause 6.2.5]

The SDP shall include bandwidth information for each media stream and also for the session in total. The bandwidth information for each media stream and for the session is defined by the Application Specific (AS) bandwidth modifier as defined in RFC 4566.

[TS 26.114, clause 7.3.1]

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556.

[TS 26.114, clause 7.4.4]

The following RTP payload format shall be used:

- T.140 text conversation RTP payload format according to RFC 4103.

Real-time text shall be the only payload type in its RTP stream because the RTP sequence numbers are used for loss detection and recovery. The redundant transmission format shall be used for keeping the effect of packet loss low.

Reference(s)

3GPP TS 24.229[10] clauses 5.1.4.1 TS 26.114 [66] clause 6.2.5, 7.3 and1, 7.4.4.

12.17.3 Test purpose

1) To verify that, when initiating MT MTSI text call and SS has resources available, the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

4) To verify that the UE is able to release the call.

12.17.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBAonly) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

GIBA (Yes/No)

Support for initiating a session (Yes/No)

Support for text (Yes/No)

Support for IMS Multimedia Telephony (Yes/No)

Test procedure

1) Execute annex C.13

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-10			Steps defined in annex C.13	MTSI MT text call

NOTE: The default messages contents in annex A are used with condition 'IMS security' or 'GIBA' when applicable

Specific Message Content

-

12.17.5 Test requirements

The UE shall send requests and responses as described in clause 12.17.4

12.18 MTSI MO speech call / SSAC / 0% access probability for MTSI MO speech call

12.18.1 Definition and applicability

Test to verify that the UE does not initiate an audio session under access barring for MTSI MO speech call. This process is described in 3GPP TS 24.173[65]. The test case is applicable for IMS security or GIBA.

12.18.2 Conformance requirement

[TS 24.173, clause J.2.1.1]:

The following information is provided by lower layer:

- BarringFactorForMMTEL-Voice: barring rate for MMTEL voice;
- BarringTimeForMMTEL-Voice: barring timer for MMTEL voice;

…

Upon request from a user to establish a multimedia telephony communication session as described in subclause 5.2, the UE shall:

1) if the multimedia telephony communication session to be established is an emergency session, then skip the rest of steps below and continue with session establishment as described in subclause 5.2;
2) retrieve SSAC related information mentioned above from lower layers;
3) if video is offered in the multimedia telephony communication session:

…

4) if audio is offered in the multimedia telephony communication session:

   A) if back-off timer Ty is running, reject the multimedia telephony communication session establishment and skip the rest of steps below; or

   B) else, then;

      I) draw a new random number "rand3" that is uniformly distributed in the range $0 \leq rand3 < 1$; and

      II) if the random number "rand3" is lower than BarringFactorForMMTEL-Voice, then skip the rest of steps below and continue with session establishment as described in subclause 5.2;

      III) else, then;

         i) draw a new random number "rand4" that is uniformly distributed in the range $0 \leq rand4 < 1$; and

         ii) start timer Ty with the timer value calculated using the formula:

         Ty = (0,7 + 0,6*rand4) * BarringTimeForMMTEL-Voice; and

         iii) reject the multimedia telephony communication session establishment;

Reference(s)

3GPP TS 24.173[65], clause J.2.1.1.

12.18.3 Test purpose

1) To verify that the UE does not initiate an audio session under access barring for MTSI MO speech call.

2) To verify that the UE does not initiate an audio session in case back-off timer Ty is running.

12.18.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated an EPS bearer context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security). SS sets *ac-BarringFactor* included in *ssac-BarringForMMTEL-Voice* to 'p00' defined in TS 36.331[114] and does not perform access class control except SSAC.

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

GIBA (Yes/No)

Support for initiating a session (Yes/No)

Support for speech (Yes/No)

Support for IMS Multimedia Telephony (Yes/No)

Test procedure

1) MO call for EPS is initiated on the UE.

2) The SS waits for 10s to check that the UE does not send the INVITE.

3) The SS sends *Paging* message including *systemInfoModification*.

4) The SS broadcasts *SystemInformationBlockType2* including no *ssac-BarringForMMTEL-Voice-r9*.

5) The UE waits for 15s to receive system information.

6) MO call for EPS is initiated on the UE.

7) The SS waits for 10s to check that the UE does not send the INVITE.

8) The UE waits for 49s to expire the timer Ty.

9-21) MO call for EPS is initiated on the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			Step 1 defined in annex C.21	MO call for EPS is initiated on the UE.
2				To verify that the UE does not send INVITE message within 10s because the random number is higher than *BarringFactorForMMTEL-Voice*. The timer Ty starts.
3	←		*Paging*	SS sends *Paging* including *systemInfoModification*.
4	←		*SystemInformationBlockType2*	SS broadcasts the *SystemInformationBlockType2* including no *ssac-BarringForMMTEL-Voice-r9*.
5				Wait for 15s for the UE to receive system information.
6			Step 1 defined in annex C.21	MO call for EPS is initiated on the UE.
7				To verify that the UE does not send INVITE message within 10s because the timer Ty is running.
8				Wait for 49s to expire the timer Ty. NOTE: The UE starts timer Ty in step2. Maximum time of timer Ty is 83.2 sec ((0.7 + 0.6 * 1) * s64). At the end of step 7, 35 sec elapses from step 2. Therefore 49 sec (84s - 35s) is enough to wait timer Ty expiry.
9-21			Steps defined in annex C.21	MTSI MO speech call for EPS.

Specific Message Contents

SystemInformationBlockType2 (initial conditions)

Use the default message in 3GPP TS 36.508[94] Table 4.4.3.3-1 with the following exceptions:

IE	Value/Remarks
- ssac-BarringForMMTEL-Voice-r9	
-- ac-BarringFactor	p00
-- ac-BarringTime	s64
-- ac-BarringForSpecialAC	11111

Paging (step 3)

Use the default message in 3GPP TS 36.508[94] Table 4.6.1-7 with the following exceptions:

IE	Value/Remarks
- pagingRecordList	Not present
- systemInfoModification	true

SystemInformationBlockType2 (step 4)

Use the default message in 3GPP TS 36.508[94] Table 4.4.3.3-1:

Steps 9 - 21 as specified in annex C.21.

12.18.5 Test requirements

At step 2 the UE shall not send the INVITE.

At step 7 the UE shall not send the INVITE.

At step 10 the UE shall send the INVITE.

12.19 MTSI MO video call / SSAC / 0% access probability for MTSI MO video call

12.19.1 Definition and applicability

Test to verify that the UE does not initiate a video session under access barring for MTSI MO video call. This process is described in 3GPP TS 24.173[65]. The test case is applicable for IMS security or GIBA.

12.19.2 Conformance requirement

[TS 24.173, clause J.2.1.1]:

The following information is provided by lower layer:

…

- BarringFactorForMMTEL-Video: barring rate for MMTEL video; and
- BarringTimeForMMTEL-Video: barring timer for MMTEL video.

Upon request from a user to establish a multimedia telephony communication session as described in subclause 5.2, the UE shall:

1) if the multimedia telephony communication session to be established is an emergency session, then skip the rest of steps below and continue with session establishment as described in subclause 5.2;
2) retrieve SSAC related information mentioned above from lower layers;
3) if video is offered in the multimedia telephony communication session:
   A) if back-off timer Tx is running, reject the multimedia telephony communication session establishment and skip the rest of steps below; or
   B) else, then:
      I) draw a new random number "rand1" that is uniformly distributed in the range $0 \leq rand1 < 1$; and
      II) if the random number "rand1" is lower than BarringFactorForMMTEL-Video, then skip the rest of steps below and continue with session establishment as described in subclause 5.2;
      III) else, then;
         i) draw a new random number "rand2" that is uniformly distributed in the range $0 \leq rand2 < 1$; and
         ii) start back-off timer Tx with the timer value calculated using the formula:

         Tx = (0,7 + 0,6*rand2) * BarringTimeForMMTEL-Video; and

         iii) reject the multimedia telephony communication session establishment and skip the rest of steps below;

Reference(s)

3GPP TS 24.173[65], clause J.2.1.1.

12.19.3 Test purpose

1) To verify that the UE does not initiate a video session under access barring for MTSI MO video call.
2) To verify that the UE does not initiate a video session in case back-off timer Tx is running.
3) To verify that the UE initiates a video session after back-off timer Tx expires.

12.19.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated an EPS bearer context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security). SS sets *ac-BarringFactor* included in *ssac-BarringForMMTEL-Video* to "p00" defined in TS 36.331[114] and does not perform access class control except SSAC.

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

GIBA (Yes/No)

Support for initiating a session (Yes/No)

Support for video (Yes/No)

Support for IMS Multimedia Telephony (Yes/No)

UE supports end-to-access-edge media security using SDES (Yes/No)

Test procedure

1) MO MTSI video call for EPS is initiated on the UE.

2) The SS waits for 10s to check that the UE does not send the INVITE.

3) The SS sends *Paging* message including *systemInfoModification*.

4) The SS broadcasts *SystemInformationBlockType2* including no *ssac-BarringForMMTEL-Video-r9*.

5) The UE waits for 15s to receive system information.

6) MO MTSI video call for EPS is initiated on the UE.

7) The SS waits for 10s to check that the UE does not send the INVITE.

8) The UE waits for 49s to expire the timer Tx.

9-21) UE executes the procedures of annex C.25 for setting up MTSI video call for EPS.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			Step 1 defined in annex C.25	MO call for EPS is initiated on the UE.
2				To verify that the UE does not send INVITE message within 10s because the random number is higher than *BarringFactorForMMTEL-Video*. The timer Tx starts.
3	←		*Paging*	SS sends *Paging* including *systemInfoModification*.
4	←		*SystemInformationBlockType2*	SS broadcasts the *SystemInformationBlockType2* including no *ssac-BarringForMMTEL-Video-r9*.
5				Wait for 15s for the UE to receive system information.
6			Step 1 defined in annex C.25	MO call for EPS is initiated on the UE.
7				To verify that the UE does not send INVITE message within 10s because the timer Tx is running.
8				Wait for 49s to expire the timer Tx. NOTE: The UE starts timer Tx in step2. Maximum time of timer Tx is 83.2 sec ((0.7 + 0.6 * 1) * s64). At the end of step 7, 35 sec elapses from step 2. Therefore 49 sec (84s - 35s) is enough to wait timer Tx expiry.
9-21			Steps defined in annex C.25	MTSI MO video call for EPS.

Specific Message Contents

SystemInformationBlockType2 (initial conditions)

Use the default message in 3GPP TS 36.508[94] Table 4.4.3.3-1 with the following exceptions:

IE	Value/Remarks
- ssac-BarringForMMTEL-Video-r9	
-- ac-BarringFactor	p00
-- ac-BarringTime	s64
-- ac-BarringForSpecialAC	11111

Paging (step 3)

Use the default message in 3GPP TS 36.508[94] Table 4.6.1-7 with the following exceptions:

IE	Value/Remarks
- pagingRecordList	Not present
- systemInfoModification	true

SystemInformationBlockType2 (step 4)

Use the default message in 3GPP TS 36.508[94] Table 4.4.3.3-1:

Steps 9 - 21 as specified in annex C.25.

12.19.5 Test requirements

At step 2 the UE shall not send the INVITE.

At step 7 the UE shall not send the INVITE.

At step 10 the UE shall send the INVITE.

12.20 Emergency call / Success / SSAC / 0% access probability for MTSI MO speech call

12.20.1 Definition and applicability

Test to verify that the UE performs the IMS emergency call under access barring for MTSI MO speech call and access class barring for MO data in E-UTRA. The process consists of setting up EPS emergency bearers, sending initial emergency registration to S-CSCF via the P-CSCF discovered, authenticating the user and finally initiating the IMS emergency call. The test case is applicable for IMS security.

12.20.2 Conformance requirement

[TS 24.173 clause 5.2]:

The IMS multimedia telephony communication service can support different types of media, including media types listed in 3GPP TS 22.173 [2]. The session control procedures for the different media types shall be in accordance with 3GPP TS 24.229 [13] and 3GPP TS 24.247 [14], with the following additions:

[TS 24.173 clause J.2.1.1]:

The following information is provided by lower layer:

- BarringFactorForMMTEL-Voice: barring rate for MMTEL voice;
- BarringTimeForMMTEL-Voice: barring timer for MMTEL voice;
- BarringFactorForMMTEL-Video: barring rate for MMTEL video; and
- BarringTimeForMMTEL-Video: barring timer for MMTEL video.

Upon request from a user to establish a multimedia telephony communication session as described in subclause 5.2, the UE shall:

1) if the multimedia telephony communication session to be established is an emergency session, then skip the rest of steps below and continue with session establishment as described in subclause 5.2;

[TS 24.229 clause 5.1.6.2]:

When the user initiates an emergency call, if emergency registration is needed (including cases described in subclause 5.1.6.2A), the UE shall perform an emergency registration prior to sending the SIP request related to the emergency call.

The UE shall have only one valid emergency registration at any given time. If the UE initiates a new emergency registration using different contact address, and the previous emergency registration has not expired, the UE shall consider the previous emergency registration as expired.

...

When a UE performs an initial emergency registration the UE shall perform the actions as specified in subclause 5.1.1.2 with the following additions and modifications:

a) the UE shall include a "sos" SIP URI parameter in the Contact header field as described in subclause 7.2A.13, indicating that indicates that this is an emergency registration and that the associated contact address is allowed only for emergency service; and

b) the UE shall populate the From and To header fields of the REGISTER request with:

   - the first entry in the list of public user identities provisioned in the UE;
   - the default public user identity obtained during the normal registration, if the UE is not provisioned with a list of public user identities, but the UE is currently registered to the IM CN subsystem; and
   - the derived temporary public user identity, in all other cases.

Reference(s)

3GPP TS 24.173[65] clause 5.2 and J.2.1.1 (release 9)

3GPP TS 24.229[10] clause 5.1.6.2 (release 9)

12.20.3 Test purpose

1) To verify that the UE perform the IMS emergency call under access barring for MTSI MO speech call and access class barring for MO data in E-UTRA.

12.20.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17]. SS sets *ac-BarringFactor* included in *ssac-BarringForMMTEL-Voice* to '*p00*' and *ac-BarringFactor* included in *ac-BarringForMO-Data* to '*p00*' defined in TS 36.331[114].

UE is registered to IMS services, by executing the generic test procedure in Annex C.2. During the E-UTRA attach procedure SS has indicated to the UE that the cell supports E-UTRA emergency bearers.

Related ICS/IXIT Statement(s)

UE supports IMS emergency services (Yes/No)

UE supports IPSec ESP confidentiality protection (Yes/No)

IMS security (Yes/No)

obtaining and using GRUUs in the Session Initiation Protocol (SIP) (Yes/No)

Test procedure

1-12) IMS emergency call is initiated on the UE. UE executes the procedures of TS 36.508[94] table 4.5A.4.3-1(steps 1 to 12) for EPS emergency bearer context activation.

13-16) UE executes the procedures of annex C.20 for subsequent IMS emergency registration.

17-19) UE executes the procedures of TS 36.508[94] table 4.5A.4.3-1(steps 13 to 15) for EPS emergency bearer context activation.

20-24) UE executes the procedures of annex C.22 for setting up the emergency call for EPS.

25) Call is released on the UE. SS waits the UE to send a BYE request.

26) SS responds to the BYE request with valid 200 OK responses.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-12				RRC connection establishment of emergency call according TS 36.508 [94] table 4.5A.4.3-1.
13-16			Steps defined in annex C.20	Subsequent IMS emergency registration by the UE
17-19				Steps 13 to 15 of the generic EUTRA/EPC procedure for emergency call (TS 36.508 [94] 4.5A.4.3-1) are executed to establish the dedicated bearer associated with the default bearer used for emergency IMS signalling.
20-24			Steps defined in annex C.22	IMS emergency call for EPS setup
25	→		BYE	The UE releases the call with BYE
26	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

SystemInformationBlockType2 (initial conditions)

Use the default message in 3GPP TS 36.508[94] Table 4.4.3.3-1 with the following exceptions:

IE	Value/Remarks
- ac-BarringInfo	
-- ac-BarringForEmergency	False
-- ac-BarringForMO-Signalling	Not present
-- ac-BarringForMO-Data	
--- ac-BarringFactor	p00
--- ac-BarringTime	s4
--- ac-BarringForSpecialAC	11111
- ssac-BarringForMMTEL-Voice-r9	
-- ac-BarringFactor	p00
-- ac-BarringTime	s4
-- ac-BarringForSpecialAC	11111

INVITE (Step 20 i.e. step 1 of Annex C.22)

Use the default message 'INVITE for MO call setup' in annex A.2.1 with the following conditions:

- A7 'INVITE for creating an emergency session within an emergency registration' shall apply.

BYE (Step 25)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE (Step 26)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

12.20.5 Test requirements

At step 20, the UE shall send the INVITE.

12.21 MO MTSI Video call

12.21.1 Definition and applicability

Test to verify that the UE correctly performs IMS mobile originated video call setup and release when using IMS Multimedia Telephony with preconditions. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1, TS 24.173 [65] and TS 26.114 [66]. The test case is applicable for IMS security or GIBA.

12.21.2 Conformance requirement

[TS 24.229, clause 6.1.1]:

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 as updated by RFC 4032.

In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.

During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261.

...

For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor and the "AS" bandwidth modifier in the SDP.

...

If the media line in the SDP indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556, then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in subclause 6.1 of RFC 3890.

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in 3GPP TS 29.208.

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifier will typically get the value of zero.

The UE shall include the MIME subtype "telephone-event" in the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 4733.

The UE shall inspect the SDP contained in any SIP request or response, looking for possible indications of grouping of media streams according to RFC 3524 and perform the appropriate actions for IP-CAN bearer establishment for media according to IP-CAN specific procedures (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

If resource reservation is needed, the UE shall start reserving its local resources whenever it has sufficient information about the media streams, media authorization and used codecs available.

NOTE 2: Based on this resource reservation can, in certain cases, be initiated immediately after the sending or receiving of the initial SDP offer.

...

[TS 24.229, clause 6.1.2]:

An INVITE request generated by a UE shall contain a SDP offer and at least one media description. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session.

If the desired QoS resources for one or more media streams have not been reserved at the UE when constructing the SDP offer, the UE shall:

- indicate the related local preconditions for QoS as not met, using the segmented status type, as defined in RFC 3312 and RFC 4032, as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1); and,

- set the related media streams to inactive, by including an "a=inactive" line, according to the procedures described in RFC 4566, unless the UE knows that the precondition mechanism is supported by the remote UE.

NOTE 1: When setting the media streams to the inactive mode, the UE can include in the first SDP offer the proper values for the RS and RR modifiers and associate bandwidths to prevent the receiving of the RTCP packets, and not send any RTCP packets.

If the desired QoS resources for one or more media streams are available at the UE when the initial SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 and RFC 4032, as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1).

NOTE 2: If the originating UE does not support the precondition mechanism it will not include any precondition information in SDP.

...

Upon generating the SDP offer for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the UE shall include SDP payload containing a subset of the allowed media types, codecs and other parameters from the SDP payload of all 488 (Not Acceptable Here) responses related to the same session establishment attempt (i.e. a set of INVITE requests used for the same session establishment). The UE shall order the codecs in the SDP payload according to the order of the codecs in the SDP payload of the 488 (Not Acceptable Here) response.

NOTE 3: The UE can attempt a session establishment through multiple networks with different policies and potentially can need to send multiple INVITE requests and receive multiple 488 (Not Acceptable Here) responses from different CSCF nodes. The UE therefore takes into account the SDP contents of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE request.

Upon confirming successful local resource reservation, the UE shall create a SDP offer in which:

- the related local preconditions are set to met, using the segmented status type, as defined in RFC 3312 and RFC 4032; and

- the media streams previously set to inactive mode are set to active (sendrecv, sendonly or recvonly) mode.

Upon receiving an SDP answer, which includes more than one codec for one or more media streams, the UE shall send an SDP offer at the first possible time, selecting only one codec per media stream.

[TS 26.114 Rel-8, clause 5.2.2]

MTSI clients in terminals offering video communication shall support:

- ITU-T Recommendation H.263 [22] Profile 0 Level 45.

In addition they should support:

- ITU-T Recommendation H.263 [22] Profile 3 Level 45;

- MPEG-4 (Part 2) Visual [23] Simple Profile Level 3with the following constraints:

  - Number of Visual Objects supported shall be limited to 1.

  - The maximum frame rate shall be 30 frames per second.

  - The maximum f_code shall be 2.

  - The intra_dc_vlc_threshold shall be 0.

  - The maximum horizontal luminance pixel resolution shall be 352 pels/line.

- The maximum vertical luminance pixel resolution shall be 288 pels/VOP.

- If AC prediction is used, the following restriction applies: QP value shall not be changed within a VOP (or within a video packet if video packets are used in a VOP). If AC prediction is not used, there are no restrictions to changing QP value.

- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Baseline Profile Level 1.1 with constraint_set1_flag=1 and without requirements on output timing conformance (annex C of [24]). Each sequence parameter set of H.264 (AVC) shall contain the vui_parameters syntax structure including the num_reorder_frames syntax element set equal to 0.

[TS 26.114 Rel-10, clause 5.2.2]

MTSI clients in terminals offering video communication shall support:

- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Constrained Baseline Profile (CBP) Level 1.2.

In addition they should support:

- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Constrained Baseline Profile Level 3.1.

In addition they may support:

- ITU-T Recommendation H.263 [22] Profile 0 Level 45.

[TS 26.114, clause 6.2.1a2]:

For voice and real-time text, SDPCapNeg shall be used when offering AVPF the first time for a new media type in the session since the support for AVPF in the answering client is not known at this stage. For video, an MTSI client shall either offer AVPF and AVP together using SDPCapNeg, or the MTSI client shall offer only AVPF, without using SDPCapNeg. If an MTSI client has offered only AVPF for video, and then receives as response either an SDP answer where the video media component has been rejected, or an SIP 488 or 606 failure response with an SDP body indicating that only AVP is supported for video media, the MTSI client should send a new SDP offer with AVP as transport for video. Subsequent SDP offers, in a re-INVITE or UPDATE, may offer AVPF without SDPCapNeg if it is known from an earlier re-INVITE or UPDATE that the answering client supports this RTP profile. If the offer includes only AVP then SDPCapNeg does not need to be used, which can occur for: text; speech if RTCP is not used; and in re-INVITEs or UPDATEs where the RTP profile has already been negotiated for the session in a preceding INVITE or UPDATE.

When offering AVP and AVPF using SDPCapNeg, the MTSI client shall offer AVP on the media (m=) line and shall offer AVPF using SDPCapNeg mechanisms. The SDPCapNeg mechanisms are used as follows:

- The support for AVPF is indicated in an attribute (a=) line using the transport capability attribute "tcap". AVPF shall be preferred over AVP.

- At least one configuration using AVPF shall be listed using the attribute for potential configurations "pcfg".

[TS 26.114, clause 6.2.3]:

If video is used in a session, the session setup shall determine the bandwidth, RTP profile, video codec, profile and level. The "imageattr" attribute as specified in [76] should be supported.

An MTSI client shall offer AVPF for all media streams containing video. RTP profile negotiation shall be done as described in clause 6.2.1a.

Examples of SDP offers and answers for video can be found in clause A.4.

NOTE: For H.264 / MPEG-4 (Part 10) AVC, the optional max-rcmd-nalu-size receiver-capability parameter of RFC 3984 [25] should be set to the smaller of the MTU size (if known) minus header size or 1 400 bytes (otherwise).

[TS 26.114, clause 7.3.1]:

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556 . Therefore, an MTSIclient shall include the "b=RS:" and "b=RR:" fields in SDP, and shall be able to interpret them. There shall be an upper limit on the allowed RTCP bandwidth for each RTP session signalled by the MTSI client. This limit is defined as follows:

- 4 000 bps for the RS field (at media level);
- 3 000 bps for the RR field (at media level).

Reference(s)

3GPP TS 24.229[10], clauses 6.1.1 and 6.1.2, and TS 26.114 [66], clauses 5.2.2, 6.2.1a2, 6.2.3 and 7.3.1.

12.21.3 Test purpose

1) To verify that when initiating MO video call the UE performs correct exchange of SIP protocol signalling messages for setting up the session; and
2) To verify that within SIP signalling the UE performs the correct exchange of SDP messages for negotiating media and indicating preconditions for resource reservation (as described by 3GPP TS 24.229 [10], clause 6.1).
3) To verify that the UE is able to release the video call.

12.21.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Related ICS/IXIT Statement(s)

- Support for initiating a session (Yes/No)
- Support for IMS Multimedia Telephony (Yes/No)
- Support for speech (Yes/No)
- Support for video (Yes/No)
- Support for integration of resource management and SIP (use of preconditions) (Yes/No)
- IMS security (Yes/No)
- GIBA (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-15) UE executes the procedures described in TS 36.508 [94] table 4.5A.8.3-1, steps 1 to 15.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-13			Steps defined in annex C.25	MTSI MO video call. Referred from 36.508 [94] table 4.5A.8.3-1 for a UE with E-UTRA support.
14	→		BYE	The UE releases the call with BYE
15	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

Steps 1 - 13 as specified in annex C.25

BYE (Step 14)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE (Step 15)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

12.21.5 Test requirements

SS must check that if the UE uses IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

Step 14: the UE shall send a BYE request with the correct content, according to common message definitions

12.22 MT MTSI Video call

12.22.1 Definition and applicability

Test to verify that the UE correctly performs IMS mobile terminated video call setup when using IMS Multimedia Telephony. This process is described in 3GPP TS 24.229 [10], clauses 5.1.3 and 6.1, TS 24.173 [65] and TS 26.114 [66]. The test case is applicable for IMS security or GIBA.

12.22.2 Conformance requirement

[TS 24.229, clause 5.1.4.1]

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires local resource reservation.

NOTE 1: The terminating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

If local resource reservation is required at the terminating UE and the terminating UE supports the precondition mechanism, and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header or Require header, the terminating UE shall make use of the precondition mechanism and shall indicate a Require header with the "precondition" option-tag in any response or subsequent request it sends towards to the originating UE; or

…

If local resource reservation is not required by the terminating UE andthe terminating UE supports the precondition mechanism and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header and:

- the required resources at the originating UE are not reserved, the terminating UE shall use the precondition mechanism; or

[TS 24.229, clause 6.1.3]

If the terminating UE had previously set one or more media streams to inactive mode and the QoS resources for those media streams are now ready, it shall set the media streams to active mode by applying the procedures described in RFC 4566 with respect to setting the direction of media streams.

…

Upon sending a SDP answer to an SDP offer, with the SDP answer including one or more media streams for which the originating side did indicate its local preconditions as not met, if the precondition mechanism is supported by the terminating UE, the terminating UE shall indicate its local preconditions and request the confirmation for the result of the resource reservation at the originating end point.

[TS 26.114 Rel-8, clause 5.2.2]

MTSI clients in terminals offering video communication shall support:

- ITU-T Recommendation H.263 [22] Profile 0 Level 45.

In addition they should support:

- ITU-T Recommendation H.263 [22] Profile 3 Level 45;
- MPEG-4 (Part 2) Visual [23] Simple Profile Level 3with the following constraints:
  - Number of Visual Objects supported shall be limited to 1.
  - The maximum frame rate shall be 30 frames per second.
  - The maximum f_code shall be 2.
  - The intra_dc_vlc_threshold shall be 0.
  - The maximum horizontal luminance pixel resolution shall be 352 pels/line.
  - The maximum vertical luminance pixel resolution shall be 288 pels/VOP.
  - If AC prediction is used, the following restriction applies: QP value shall not be changed within a VOP (or within a video packet if video packets are used in a VOP). If AC prediction is not used, there are no restrictions to changing QP value.
- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Baseline Profile Level 1.1 with constraint_set1_flag=1 and without requirements on output timing conformance (annex C of [24]). Each sequence parameter set of H.264 (AVC) shall contain the vui_parameters syntax structure including the num_reorder_frames syntax element set equal to 0.

[TS 26.114 Rel-10, clause 5.2.2]

MTSI clients in terminals offering video communication shall support:

- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Constrained Baseline Profile (CBP) Level 1.2.

In addition they should support:

- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Constrained Baseline Profile Level 3.1.

In addition they may support:

- ITU-T Recommendation H.263 [22] Profile 0 Level 45.

[TS 26.114, clause 6.2.1a3]:

An invited MTSI client should accept using AVPF whenever supported. If AVPF has been offered using SDPCapNeg and is to be used in the session then the MTSI client shall:

- select one configuration out of the potential configurations defined in the SDP offer for using AVPF;
- indicate in the media (m=) line of the SDP answer that the profile to use is AVPF; and
- indicate the selected configuration for using AVPF in the attribute for actual configurations "acfg".

If AVP is to be used then the MTSI shall not indicate any SDPCapNeg attributes for using AVPF in the SDP answer.

[TS 26.114, clause 6.2.3]:

If video is used in a session, the session setup shall determine the bandwidth, RTP profile, video codec, profile and level. The "imageattr" attribute as specified in [76] should be supported.

An MTSI client shall offer AVPF for all media streams containing video. RTP profile negotiation shall be done as described in clause 6.2.1a.

Examples of SDP offers and answers for video can be found in clause A.4.

NOTE: For H.264 / MPEG-4 (Part 10) AVC, the optional max-rcmd-nalu-size receiver-capability parameter of RFC 3984 [25] should be set to the smaller of the MTU size (if known) minus header size or 1 400 bytes (otherwise).

[TS 26.114, clause 6.2.5]

The SDP shall include bandwidth information for each media stream and also for the session in total. The bandwidth information for each media stream and for the session is defined by the Application Specific (AS) bandwidth modifier as defined in RFC 4566.

[TS 26.114, clause 7.3.1]

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556.

Reference(s)

3GPP TS 24.229[10] clauses 5.1.4.1, 6.1.3, TS 26.114 [66] clause 5.2.2, 6.2.1a3,6.2.3, 6.2.5 and 7.3.1.

12.22.3 Test purpose

1) To verify that, when initiating MT MTSI video call and SS needs to reserve resources, the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

4) To verify that the UE is able to release the call.

12.22.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipp5ed into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

GIBA (Yes/No)

Support for initiating a session (Yes/No)

Support for speech (Yes/No)

Support for video (Yes/No)

Support for IMS Multimedia Telephony (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-27) UE executes the procedures described in TS 36.508 [94] table 4.5A.9.3-1, steps 1 to 27.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-15			Steps defined in annex C.26	MTSI MT video call. Referred from 36.508 [94] table 4.5A.9.3-1 for a UE with E-UTRA support.

NOTE: The default messages contents in annex A are used with condition 'IMS security' or 'GIBA' when applicable

Specific Message Content

None.

12.22.5 Test requirements

The UE shall send requests and responses as described in clause 12.22.4

13 Signalling Compression (SIGComp)

13.1 SigComp in the Initial registration

Editor"s note: This test case needs to be updated to Release-8.

13.1.1 Definition and applicability

Test to verify that the UE can correctly register to IMS services when the P-CSCF supports and uses SigComp. This includes correct decompression by the UE and optional compression by the UE. The test case is applicable for IMS security.

13.1.2 Conformance requirement

The UE shall support SigComp as specified in RFC 3320. When using SigComp the UE shall send compressed SIP messages in accordance with RFC 3486.

…

The UE shall support the SIP dictionary specified in RFC 3485. If compression is enabled, the UE shall use the dictionary to compress the first message.

…

The UE should compress the requests and responses transmitted to the P-CSCF according to subclause 8.1.1.

NOTE 1: Compression of SIP messages is an implementation option. However, compression is strongly recommended.

NOTE 2: Since compression support is mandatory, the UE may send even the first message compressed. Sigcomp provides mechanisms to allow the UE to know if state has been created in the P-CSCF or not.

…

The UE shall decompress the compressed requests and responses received from the P-CSCF according to subclause 8.1.1.

Reference(s)

3GPP TS 24.229 [10], clauses 8.1.1, 8.1.2 and 8.1.3.

13.1.3 Test purpose

1) To verify that the UE performs initial registration, subscription and notification according to 3GPP TS 24.229 [10]. The UE can send messages compressed or not compressed. The UE can announce to support SIP Compression 'comp=sigcomp'; and

2) To verify that the UE uses the SIP/SDP dictionary specified in RFC 3485 [25] at least in the first message sent;; and

3) To verify that the UE decompresses all the SIP messages sent by the SS in accordance 3GPP TS 24.229 [10] clause 8.1.1. This is tested implicitly by checking the messages sent by the UE verifying the correct exchange of SIP protocol signalling messages.

NOTE: The presence of the SIP Compression announcement 'comp=sigcomp' by either UE and P-CSCF indicates the willingness to send or receive SIP messages compressed. The mechanism which controls the willingness to apply SigComp is described in RFC 3486 [26] by sentences containing SHOULD, for this reason the presence of the 'comp=sigcomp' parameter from UE side (even if strongly recommended and consistent with the use of compression) is considered optional.

13.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services, but has an active PDP context and has discovered the SS as P-CSCF by executing the generic test procedure in Annex C.2 up to step 3.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

Indicate Sigcomp (Yes/No)

Test procedure

1) IMS registration is initiated on the UE. The SS waits for the UE to send an initial REGISTER request. The SIP Compression announcement 'comp=sigcomp' in the Via header and in the Contact header may be included. The message can be sent compressed or not compressed.

2) The SS responds to the initial REGISTER request with a compressed valid 401 Unauthorized response, headers populated according to the 401 response common message definition.

3) The SS waits for the UE to set up a temporary set of security associations and send another REGISTER request over those security associations. The SIP Compression announcement 'comp=sigcomp' in the Via header and in the Contact header may be included. The message can be sent compressed or not compressed.

4) The SS responds to the second REGISTER request with a valid compressed 200 OK response, sent over the same temporary set of security associations that the UE used for sending the REGISTER request. The SS shall

populate the headers of the 200 OK response according to the 200 response for REGISTER common message definition.

5) The SS waits for the UE to send a SUBSCRIBE request. The SIP Compression announcement 'comp=sigcomp' in the Via and in the Contact header may be included. The message can be sent compressed or not compressed.

6) The SS responds to the SUBSCRIBE request with a valid compressed 200 OK response, headers populated according to the 200 response for SUBSCRIBE common message definition with the SIP Compression announcement 'comp=sigcomp' in the record-route header.

7) The SS sends a compressed NOTIFY request for the subscribed registration event package. In the request the Request URI, headers and the request body shall be populated according to the NOTIFY common message definition.

8) The SS waits for the UE to respond to the NOTIFY with a 200 OK response. The message can be sent compressed or not compressed.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	The UE sends initial registration for IMS services. with comp=sigcomp in the Via and Contact headers. The message can be sent compressed or not compressed.
2	←		401 Unauthorized	The SS responds with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network. This message is sent compressed.
3	→		REGISTER	The UE completes the security negotiation procedures, sets up a temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials. The message can be sent compressed or not compressed.
4	←		200 OK	The SS responds with 200 OK. This message is sent compressed.
5	→		SUBSCRIBE	The UE subscribes to its registration event package. The message can be sent compressed or not compressed.
6	←		200 OK	The SS responds with 200 OK. This message is sent compressed.
7	←		NOTIFY	The SS sends initial NOTIFY for registration event package, containing full registration state information for the registered public user identity in the XML body. This message is sent compressed.
8	→		200 OK	The UE responds with 200 OK. The message can be sent compressed or not compressed.

Specific Message Contents

REGISTER (Step 1)

Use the default message 'REGISTER' in annex A.1.1, condition A1 "Initial unprotected REGISTER". The following exceptions can be used if the UE is willing to receive response and request compressed:

Header/param	Value/remark
Via	
via-compression	comp=sigcomp
Contact	
compression-param	comp=sigcomp

401 Unauthorized for REGISTER (Step 2)

Use the default message '401 Unauthorized for REGISTER' in annex A.1.2.

REGISTER (Step 3)

Use the default message 'REGISTER' in annex A.1.1, condition A2 "Subsequent REGISTER sent over security associations". The following exceptions can be used if the UE is willing to receive response and request compressed:

Header/param	Value/remark
Via	
via-compression	comp=sigcomp
Contact	
compression-param	comp=sigcomp

200 OK for REGISTER (Step 4)

Use the default message '200 OK for REGISTER' in annex A.1.3.

SUBSCRIBE (Step 5)

Use the default message 'SUBSCRIBE for reg-event package' in annex A.1.4. The following exceptions can be used if the UE is willing to receive response and request compressed:

Header/param	Value/remark
Via	
via-compression	comp=sigcomp
Contact	
compression-param	comp=sigcomp

200 OK for SUBSCRIBE (Step 6)

Use the default message '200 OK for SUBSCRIBE' in annex A.1.5 with the following exceptions:

Header/param	Value/remark
Record-Route	
compression-param	comp=sigcomp

NOTIFY (Step 7)

Use the default message 'NOTIFY for reg-event package' in annex A.1.6 with the following exceptions:

Header/param	Value/remark
Via	
via-parm1:	
via-compression	comp=sigcomp

200 OK for NOTIFY (Step 8)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

13.1.5 Test requirements

Step 1: SS shall check that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends initial REGISTER request. If the message has been sent compressed then check the following:

a) the message is sent compressed according to RFC 3320 [24]; and

b) if the message received from the UE is the first compressed message, then the compression shall support SIP dictionary specified in RFC 3485 [25]; and

Step 3: SS shall check that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends second REGISTER request. If the message has been sent compressed then check the following:

a) the message is sent compressed according to RFC 3320 [24]; and

b) if the message received from the UE is the first compressed message, then the compression shall support SIP dictionary specified in RFC 3485 [25]; and

Step 5: SS shall check that, in accordance to the 3GPP TS 24.229 [10] clause 8.1.1, the UE sends a SUBSCRIBE request. If the message has been sent compressed then check the following:

a) the message is sent compressed according to RFC 3320 [24]; and

b) if the message received from the UE is the first compressed message, then the compression shall support SIP dictionary specified in RFC 3485 [25]; and

Step 8: SS shall check that, in accordance to the 3GPP TS 24.229 [10] clause 8.1.1, the UE sends a 200 OK for NOTIFY response. If the message has been sent compressed then check the following:

a) the message is sent compressed according to RFC 3320 [24]; and;

b) if the message received from the UE is the first compressed message, then the compression shall support SIP dictionary specified in RFC 3485 [25].

13.2 SigComp in the MO Call

Editor"s note: This test case needs to be updated to Release-8.

13.2.1 Definition and applicability

Test to verify that the UE correctly performs IMS mobile originated call setup when the P-CSCF supports and uses SigComp. This includes correct decompression and optional compression by the UE.

13.2.2 Conformance requirement

The UE shall support SigComp as specified in RFC 3320. When using SigComp the UE shall send compressed SIP messages in accordance with RFC 3486.

…

The UE should compress the requests and responses transmitted to the P-CSCF according to subclause 8.1.1.

NOTE 1: Compression of SIP messages is an implementation option. However, compression is strongly recommended.

NOTE 2: Since compression support is mandatory, the UE may send even the first message compressed. Sigcomp provides mechanisms to allow the UE to know if state has been created in the P-CSCF or not.

…

The UE shall decompress the compressed requests and responses received from the P-CSCF according to subclause 8.1.1.

Reference(s)

3GPPTS 24.229 [10], clauses 8.1.1, 8.1.2, and 8.1.3.

13.2.3 Test purpose

1) To verify that, when initiating MO call, the UE performs the session setup according to 3GPP TS 24.229 [10]. The UE can send messages compressed or not compressed The UE can announce to support SIP Compression 'comp=sigcomp'; and

2) To verify that the UE decompresses all the SIP messages sent by the SS in accordance 3GPP TS 24.229 [10] clause 8.1.1. This is tested implicitly by verifying the correct exchange of SIP protocol signalling messages..

NOTE: The presence of the SIP Compression announcement 'comp=sigcomp' by either UE and P-CSCF indicates the willingness to send or receive SIP messages compressed. The mechanism which controls the willingness to apply SigComp is described in RFC 3486 [26] by sentences containing SHOULD, for this reason the presence of the 'comp=sigcomp' parameter from UE side (even if strongly recommended and consistent with the use of compression) is considered optional.

13.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step (with Compression activated on SS).

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for use of preconditions (Yes/No)

Test procedure

1) MO call is initiated on the UE. SS waits the UE to send an INVITE request with first SDP offer, over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.3. The SIP Compression announcement 'comp=sigcomp' in the Via header, in the Route header and in the Contact header may be included. The request may be sent compressed.

2) The SS responds to the INVITE request with a 100 Trying response. The response is sent compressed.

3) The SS responds to the INVITE request with a 183 Session in Progress response with the SIP Compression announcement 'comp=sigcomp' in the Record-Route header. The response is sent compressed.

4) The SS waits for the UE to send a PRACK request possibly containing the second SDP offer. The SIP Compression announcement 'comp=sigcomp' in the Via header may be included and in the Route header shall be included. The request may be sent compressed.

5) The SS responds to the PRACK request with valid 200 OK response. The response is sent compressed.

6) The SS waits for the UE to optionally send a UPDATE request containing the final SDP offer. UE will not send the UPDATE request if PRACK request of step 4 already contained the final offer with preconditions met. The SIP Compression announcement 'comp=sigcomp' in the Via header may be included and in the Route header shall be included. The request may be sent compressed.

7) The SS responds to the UPDATE request (if UE sent one) with valid 200 OK response. The response is sent compressed.

8) The SS responds to the INVITE request with 180 Ringing response with the SIP Compression announcement 'comp=sigcomp' in the Record-Route header. The response is sent compressed.

9) The SS waits for the UE to send a PRACK request. The SIP Compression announcement 'comp=sigcomp' in the Via header may be included and in the Route header shall be included. The request may be sent compressed.

10) The SS responds to the PRACK request with valid 200 OK response. The response is sent compressed.

11) The SS responds to the INVITE request with valid 200 OK response with the SIP Compression announcement 'comp=sigcomp' in the Record-Route header. The response is sent compressed.

12) The SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE. The SIP Compression announcement 'comp=sigcomp' in the Route shall be included. The acknowledge message may be sent compressed.

13) Call is released on the UE. The SS waits the UE to send a BYE request. The SIP Compression announcement 'comp=sigcomp' in the Via header may be included and in the Route header shall be included. The request may be sent compressed.

14) The SS responds to the BYE request with valid 200 OK response. The response is sent compressed.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		INVITE	UE sends INVITE with the first SDP offer indicating all desired medias and codecs the UE supports. The request may be sent compressed.
2	←		100 Trying	The SS responds with a 100 Trying provisional response. The response is sent compressed.
3	←		183 Session in Progress	The SS responds with an SDP answer indicating the medias and codecs acceptable for SS. The response is sent compressed.
4	→		PRACK	UE acknowledges the receipt of 183 response with PRACK and offers second SDP. The request may be sent compressed.
5	←		200 OK	The SS responds PRACK with 200 OK. The response is sent compressed.
6	→		UPDATE	Optional step: UE sends an UPDATE. The request may be sent compressed.
7	←		200 OK	Optional step : The SS responds UPDATE with 200 OK. The response is sent compressed.
8	←		180 Ringing	The SS responds INVITE with 180. The response is sent compressed.
9	→		PRACK	UE acknowledges the receipt of 180 response by sending PRACK. The request may be sent compressed.
10	←		200 OK	The SS responds PRACK with 200 OK. The response is sent compressed.
11	←		200 OK	The SS responds INVITE with 200 OK to indicate that the virtual remote UE had answered the call. The response is sent compressed.
12	→		ACK	The UE acknowledges the receipt of 200 OK for INVITE. The acknowledge message may be sent compressed.
13	→		BYE	The UE releases the call with BYE. The request may be sent compressed.
14	←		200 OK	The SS sends 200 OK for BYE. The response is sent compressed.

Specific Message Contents

INVITE (Step 1)

Use the default message 'INVITE for MO call setup' in annex A.2.1.3 with the following exceptions:

Header/param	Value/remark
Via	
via-compression	comp=sigcomp (optional)
Route	
compression-param	comp=sigcomp (optional)
Contact	
compression-param	comp=sigcomp (optional)

100 Trying for INVITE (Step 2)

Use the default message '100 Trying for INVITE' in annex A.2.2.

183 Session in Progress for INVITE (Step 3)

Use the default message '183 Session in Progress for INVITE' in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Record-Route	The Compression parameter is included in the last route parameter
compression-param	comp=sigcomp

PRACK (Step 4)

Use the default message 'PRACK' in annex A.2.4 with the following exceptions:

Header/param	Value/remark
Via	
via-compression	comp=sigcomp (optional)
Route	The Compression parameter is included in the first route parameter
compression-param	comp=sigcomp (optional)

200 OK for PRACK (Step 5)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type	header shall be present only if there is SDP in message-body
media-type	*application/sdp*
Content-Length	
value	length of message-body
Message-body	SDP body of the 200 response copied from the received PRACK, if it contained one but otherwise omitted. The copied SDP body are modified, but the modifications on SDP body are out of this test case scope.

UPDATE (Step 6) optional step used when PRACK contained a=curr:qos local none

Use the default message 'UPDATE' in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Via	
via-compression	comp=sigcomp (optional)
Route	The Compression parameter is included in the first route parameter
compression-param	comp=sigcomp (optional)

200 OK for UPDATE (Step 7) - optional step used when UE sent UPDATE

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	*application/sdp*
Content-Length value	length of message-body
Message-body	SDP body of the 200 response copied from the received UPDATE but modified. The modifications on SDP body are out of this test case scope.

180 Ringing for INVITE (Step 8)

Use the default message '180 Ringing for INVITE' in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Record-Route compression-param	The Compression parameter is included in the last route parameter comp=sigcomp

PRACK (Step 9)

Use the default message 'PRACK' in annex A.2.4 with the following exceptions:

Header/param	Value/remark
Via via-compression	comp=sigcomp (optional)
Route compression-param	The Compression parameter is included in the first route parameter comp=sigcomp (optional)

200 OK for PRACK (Step 10)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

200 OK for INVITE (Step 11)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

ACK (Step 12)

Use the default message 'ACK' in annex A.2.7 with the following exceptions:

Header/param	Value/remark
Route compression-param	The Compression parameter is included in the first route parameter comp=sigcomp (optional)

BYE (Step 13)

Use the default message 'BYE' in annex A.2.8 with the following exceptions:

Header/param	Value/remark
Via via-compression	comp=sigcomp (optional)
Route compression-param	The Compression parameter is included in the first route parameter comp=sigcomp (optional)

200 OK for BYE (Step 14)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

13.2.5 Test requirements

Step 1: The SS shall check, if the request has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends initial INVITE request as follows:

a) the request is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent response and request compressed the message content shall be in accordance to the specific message content; and

...

Step 4: The SS shall check, if the request has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends a PRACK request as follows:

a) the request is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent response and request compressed the message content shall be in accordance to the specific message content; and

...

Step 6: The SS shall check, in the case the UE may conditionally send an UPDATE request and if the request has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 is sent as follows:

a) the message is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent response and request compressed the message content shall be in accordance to the specific message content; and

...

Step 9: The SS shall check, if the request has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends a PRACK request as follows:

a) the message is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent response and request compressed the message content shall be in accordance to the specific message content; and

...

Step 12: The SS shall check, if the request has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends an ACK request as follows:

a) the message is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent response and request compressed the message content shall be in accordance to the specific message content; and

Step 13: The SS shall check, if the request has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends a BYE request as follows:

a) the message is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent response and request compressed the message content shall be in accordance to the specific message content.

13.3 SigComp in the MT Call

Editor"s note: This test case needs to be updated to Release-8.

13.3.1 Definition and applicability

Test to verify that the UE correctly performs IMS mobile terminated call setup when the P-CSCF supports and uses SigComp. This includes correct decompression and compression by the UE.

13.3.2 Conformance requirement

The UE shall support SigComp as specified in RFC 3320. When using SigComp the UE shall send compressed SIP messages in accordance with RFC 3486.

…

The UE should compress the requests and responses transmitted to the P-CSCF according to subclause 8.1.1.

NOTE 1: Compression of SIP messages is an implementation option. However, compression is strongly recommended.

NOTE 2: Since compression support is mandatory, the UE may send even the first message compressed. Sigcomp provides mechanisms to allow the UE to know if state has been created in the P-CSCF or not.

…

The UE shall decompress the compressed requests and responses received from the P-CSCF according to subclause 8.1.1.

Reference(s)

3GPPTS 24.229 [10], clauses 8.1.1, 8.1.2, and 8.1.3.

13.3.3 Test purpose

1) To verify that, when initiating MT call, the UE performs the session setup according to 3GPP TS 24.229 [10] with compression set to on. The UE can announce to support SIP Compression 'comp=sigcomp'; and

2) To verify that the UE decompresses all the SIP messages sent by the SS in accordance 3GPP TS 24.229 [10] clause 8.1.1. This is tested implicitly by verifying the correct exchange of SIP protocol signalling messages.

NOTE: The presence of the SIP Compression announcement 'comp=sigcomp' by either UE and P-CSCF indicates the willingness to send or receive SIP messages compressed. The mechanism which controls the willingness to apply SigComp is described in RFC 3486 [26] by sentences containing SHOULD, for this reason the presence of the 'comp=sigcomp' parameter from UE side (even if strongly recommended and consistent with the use of compression) is considered optional.

13.3.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step (with Compression activated on SS).

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Related ICS/IXIT Statement(s)

The SS is preconfigured to generate SDP offers that are compatible with the UE''s capabilities

Test procedure

1) The SS sends an INVITE request to the UE with the SIP Compression announcement 'comp=sigcomp' in the Via header and in the Record-Route header. The request is sent compressed.

2) The SS may receive 100 Trying provisional response from the UE. The Provisional response may be sent compressed.

3) The SS waits for the UE to send a 183 Session Progress provisional response. The SIP Compression announcement 'comp=sigcomp' in the Record-Route shall be included and in the Contact header may be included. The Provisional response may be sent compressed.

4) The SS sends PRACK request to the UE to acknowledge the 183 Session Progress with the SIP Compression announcement 'comp=sigcomp' in the Via header. The request is sent compressed.

5) The SS waits for the UE to send a 200 OK response for PRACK. The response may be sent compressed.

6) The SS sends UPDATE request to the UE, with SDP indicating that precondition is met on the server side with the SIP Compression announcement 'comp=sigcomp' in the Via header. The request is sent compressed.

7) The SS waits for the UE to send a 200 OK response for UPDATE, with proper SDP as answer. The response may be sent compressed.

8) The SS expects and receives 180 Ringing response from the UE. The SIP Compression announcement 'comp=sigcomp' in the Contact header may be included. The response may be sent compressed.

9) The SS sends PRACK request with the SIP Compression announcement 'comp=sigcomp' in the Via header. The request is sent compressed.

10) The SS waits for the UE to send a 200 OK response for the PRACK. The response may be sent compressed.

11) The SS waits for the UE to send a 200 OK response for the INVITE. The SIP Compression announcement 'comp=sigcomp' in the Record-Route shall be included and in the Contact header may be included. The response may be sent compressed.

12) The SS waits for the UE to send the ACK with the SIP Compression announcement 'comp=sigcomp' in the Via header. The ACK is sent compressed.

13) The SS sends BYE request to the UE with the SIP Compression announcement 'comp=sigcomp' in the Via header. The request is sent compressed.

14) The SS waits for the UE to send a 200 OK response for BYE. The SIP Compression announcement 'comp=sigcomp' in the Contact header may be included. The response may be sent compressed.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with the first SDP offer. The request is sent compressed.
2	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response. The Provisional response may be sent compressed.
3	→		183 Session Progress	The UE sends 183 response reliably with the SDP answer to the offer in INVITE. The Provisional response may be sent compressed.
4	←		PRACK	SS acknowledges the receipt of 183 from the UE. No SDP offer is included here. The request is sent compressed.
5	→		200 OK	The UE responds to PRACK with 200 OK. The response may be sent compressed.
6	←		UPDATE	SS sends an UPDATE with a second SDP offer after having reserved the resources. The request is sent compressed.
7	→		200 OK	The UE acknowledges the UPDATE with 200 OK and includes SDP answer to acknowledge its current precondition status.
8	→		180 Ringing	The UE responds to INVITE with 180 Ringing after its resource is ready. The response may be sent compressed.
9	←		PRACK	The SS acknowledges the 180 response with PRACK. The request is sent compressed.
10	→		200 OK	The UE acknowledges the PRACK with 200 OK. The response may be sent compressed.
11	→		200 OK	The UE responds to INVITE with 200 OK final response after the user answers the call. The response may be sent compressed.
12	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE. The ACK is sent compressed.
13	←		BYE	The SS sends BYE to release the call. The BYE is sent compressed.
14	→		200 OK	The UE sends 200 OK for the BYE request and ends the call. The response may be sent compressed.

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9 with the following exceptions:

Header/param	Value/remark
Via	
via-compression	comp=sigcomp
Record-Route	
compression-param	comp=sigcomp
Message-body	The SDP contains all mandatory SDP lines, as specified in SDP grammar in RFC 4566[27], the details on SDP are out of this test case scope.

100 Trying (Step 2)

Use the default message "100 Trying for INVITE" in annex A.2.2.

183 Session Progress (Step 3)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Status-Line Reason-Phrase	Not checked
Record-Route compression-param	The Compression parameter is included in the first route parameter comp=sigcomp
Contact compression-param	comp=sigcomp (optional)
Message-body	Properly generated SDP answer to the SDP offer contained in the INVITE. The details on SDP are out of this test case scope.

PRACK (step 4)

Use the default message "PRACK" in annex A.2.4 with following exceptions:

Header/param	Value/remark
Via via-compression	Comp=sigcomp
Message-body	Not Present

200 OK (Step 5)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

UPDATE (step 6)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Via via-compression	Comp=sigcomp (optional)
Message-body	Same SDP offer as in INVITE with version number in the 'o' line incremented by one. The details on SDP are out of this test case scope.

200 OK (step 7)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	application/SDP
Message-body	Same SDP answer as in 183 with version number in the 'o' line incremented by one. The details on SDP are out of this test case scope.

180 Ringing (step 8)

Use the default message "180 Ringing for INVITE" in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Status-Line	
Reason-Phrase	Not checked
Contact	
compression-param	comp=sigcomp (optional)

PRACK (step 9)

Use the default message "PRACK" in annex A.2.4 with following exceptions:

Header/param	Value/remark
Via	
via-compression	comp=sigcomp
Message-body	Not Present

200 OK (step 10)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

200 OK (step 11)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with following exceptions:

Header/param	Value/remark
Contact	
compression-param	comp=sigcomp (optional)

ACK (step 12)

Use the default message "ACK" in annex A.2.7 with following exceptions:

Header/param	Value/remark
Via	
via-compression	comp=sigcomp

BYE (step 13)

Use the default message "BYE" in annex A.2.8 with following exceptions:

Header/param	Value/remark
Via	
via-compression	comp=sigcomp

200 OK (step 14)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with following exceptions:

Header/param	Value/remark
Contact	
compression-param	comp=sigcomp (optional)

13.3.5 Test requirements

Step 2 (optional step): The SS shall check, if the message has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends 100 Trying response as follow:

a) the request is sent compressed according to RFC 3320 [24]; and

Step 3: The SS shall check, if the message has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends 183 Session Progress response as follows:

a) the request is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent request and response compressed the message content shall be in accordance to the specific message content; and

...

Step 5: The SS shall check, if the message has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends 200 OK response as follow:

a) the request is sent compressed according to RFC 3320 [24]; and

Step 7: The SS shall check, if the message has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends 200 OK response as follow:

a) the request is sent compressed according to RFC 3320 [24]; and

Step 8: The SS shall check, if the message has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends 180 Ringing response as follows:

a) the request is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent request and response compressed the message content shall be in accordance to the specific message content; and

...

Step 10: The SS shall check, if the message has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends 200 OK response as follow:

a) the request is sent compressed according to RFC 3320 [24]; and

Step 11: The SS shall check, if the message has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends 200 OK response as follows:

a) the request is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent request and response compressed the message content shall be in accordance to the specific message content; and

...

Step 14: The SS shall check, if the message has been sent compressed, that in accordance to the 3GPP TS 24.229 [10] clause 8.1.1 the UE sends 200 OK response as follows:

a) the request is sent compressed according to RFC 3320 [24]; and

b) in the case the UE is willing to receive subsequent request and response compressed the message content shall be in accordance to the specific message content.

13.4 Void

14 Emergency Service

14.1 Void

14.2 Void

15 Supplementary Services

15.1 Originating Identification Presentation

15.1.1 Definition and applicability

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Originating Identification Presentation. This process is described in 3GPP TS 24.607 [102]. The test case is applicable for IMS security or GIBA.

15.1.2 Conformance requirement

Generic requirements for Originating Identification Presentation can be found from Annexes F1 and F.2.

[TS 24.607 clause 4.2.1]:

The OIP service provides the terminating user with the possibility of receiving trusted (i.e. network-provided) identity information in order to identify the originating user.

In addition to the trusted identity information, the identity information from the originating user can include identity information generated by the originating user and in general transparently transported by the network. In the particular case where the "no screening" special arrangement does not apply, the originating network shall verify the content of this user generated identity information. The terminating network cannot be responsible for the content of this user generated identity information.

[TS 24.607 clause 4.10.1]:

The OIP service can be activated/deactivated using the active attribute of the <originating-identity-presentation> service element.

Reference(s)

3GPP TS 24.607[102], clauses 4.2.1 and 4.10.1.

15.1.3 Test purpose

1) To verify that the UE can request activation of Originating Identification Presentation with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Originating Identification Presentation; and

3) To verify that the UE can authenticate its HTTP requests.

15.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated an IPCAN bearer (e.g. PDP context or EPS bearer) with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to Annex C. 29.2.

Related ICS/IXIT Statement(s)

Support for MTSI (Yes/No)

Support for initiating a session (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Support for Originating Identification Presentation (Yes/No)

GAA XCAP authentication (Yes/No)

HTTP Digest XCAP authentication (Yes/No)

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Originating Identification Presentation, at step 7 deactivation of Originating Identification Presentation is respectively triggered at the UE.

15.1.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports either:

- HTTP Digest authentication (see Annex C.29.1 step 2, NOTE 1)

- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C. 29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <originating-identity-presentation> element with "active" attribute set as "true"

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <originating-identity-presentation> element with "active" attribute being set "false"

15.2 Originating Identification Restriction

15.2.1 Definition and applicability

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Originating Identification Restriction. This process is described in 3GPP TS 24.607 [102]. The test case is applicable for IMS security or GIBA.

15.2.2 Conformance requirement

Generic requirements for Originating Identification Restriction can be found from Annexes F1 and F.2.

[TS 24.607 clause 4.2.1]:

The OIR service is a service offered to the originating user. It restricts presentation of the originating user's identity information to the terminating user.

When the OIR service is applicable and activated, the originating network provides the destination network with the indication that the originating user's identity information is not allowed to be presented to the terminating user. In this case, no originating user's identity information shall be included in the requests sent to the terminating user. The presentation restriction function shall not influence the forwarding of the originating user's identity information within the network as part of the simulation service procedures.

[TS 24.607 clause 4.10.1]:

The OIR service can be activated/deactivated using the active attribute of the <originating-identity-presentation-restriction> service element. Activating the OIR service this way activates the temporary mode OIR service. When deactivated and not overruled by operator settings, basic communication procedures apply.

Reference(s)

3GPP TS 24.607[102], clauses 4.2.1 and 4.10.1.

15.2.3 Test purpose

1) To verify that the UE can request activation of Originating Identification Restriction with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Originating Identification Restriction; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated a PDP context with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Related ICS/IXIT Statement(s)

Support for MTSI (Yes/No)

Support for initiating a session (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Support for Originating Identification Restriction (Yes/No)

GAA XCAP authentication (Yes/No)

HTTP Digest XCAP authentication (Yes/No)

Test procedure

The generic test procedure according to annex C.29.1 is applied: At step 1 activation of Originating Identification Restriction, at step 7 deactivation of Originating Identification Restriction is respectively triggered at the UE.

15.2.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme it that the UE supports.

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1)

- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <originating-identity-presentation-restriction> element with "active" attribute set as "true"

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <originating-identity-presentation-restriction> element with "active" attribute being set "false"

15.3 Terminating Identification Presentation

15.3.1 Definition and applicability

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Terminating Identification Presentation. This process is described in 3GPP TS 24.608 [103]. The test case is applicable for IMS security or GIBA.

15.3.2 Conformance requirement

[TS 24.608 clause 4.2.1]:

The Terminating Identification Presentation (TIP) service provides the originating party with the possibility of receiving trusted information in order to identify the terminating party.

[TS 24.608 clause 4.9.1]:

The TIP service can be activated/deactivated using the active attribute of the <terminating-identity-presentation> service element.

Reference(s)

3GPP TS 24.608[103], clauses 4.2.1 and 4.9.1.

15.3.3 Test purpose

1) To verify that the UE can request activation of Terminating Identification Presentation with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Terminating Identification Presentation; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.3.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated a PDP context with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Related ICS/IXIT Statement(s)

Support for MTSI (Yes/No)

Support for initiating a session (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Support for Terminating Identification Presentation (Yes/No)

GAA XCAP authentication (Yes/No)

HTTP Digest XCAP authentication (Yes/No)

Test procedure

1) Activation of Terminating Identification Presentation is triggered at the UE.

2) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself and activate the service.

3) Deactivation of Terminating Identification Presentation is triggered at the UE.

4) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself and deactivate the Terminating Identification Presentation.

15.3.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports:

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1).

- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <terminating-identity-presentation> element with "active" attribute set as "true"

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <terminating-identity-presentation> element with "active" attribute being set "false"

15.4 Terminating Identification Restriction

15.4.1 Definition and applicability

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Terminating Identification Restriction. This process is described in 3GPP TS 24.608 [103]. The test case is applicable for IMS security or GIBA.

15.4.2 Conformance requirement

[TS 24.608 clause 4.2.1]:

The Terminating Identification Restriction (TIR) is a service offered to the terminating party which enables the terminating party to prevent presentation of the terminating identity information to originating party.

[TS 24.608 clause 4.9.1]:

The TIR service can be activated/deactivated using the active attribute of the <terminating-identity-presentation-restriction> service element. Activating the TIR service this way activates the temporary mode TIR service. When deactivated and not overruled by operator settings, basic communication procedures apply.

Reference(s)

3GPP TS 24.608[103], clauses 4.2.1 and 4.9.1.

15.4.3 Test purpose

1) To verify that the UE can request activation of Terminating Identification Restriction with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Terminating Identification Restriction; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.4.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated a PDP context with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Related ICS/IXIT Statement(s)

Support for MTSI (Yes/No)

Support for initiating a session (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Support for Terminating Identification Restriction (Yes/No)

GAA XCAP authentication (Yes/No)

HTTP Digest XCAP authentication (Yes/No)

Test procedure

1) Activation of Terminating Identification Restriction is triggered at the UE.

2) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself and activate the service.

3) Deactivation of Terminating Identification Restriction is triggered at the UE.

4) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself and deactivate the Terminating Identification Restriction.

15.4.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports :

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1).

- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <terminating-identity-presentation-restriction> element with "active" attribute set as "true"

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <terminating-identity-presentation-restriction> element with "active" attribute being set "false"

15.5 Communication Forwarding unconditional

15.5.1 Definition and applicability

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding unconditional. This process is described in 3GPP TS 24.604 [106]. The test case is applicable for IMS security or GIBA.

15.5.2 Conformance requirement

Generic requirements for Communication Forwarding can be found from Annexes F1 and F.4..

[TS 24.604, clause 4.2.1.2]:

The CFU service enables a served user to have the network redirect to another user communications which are addressed to the served user's address. The CFU service may operate on all communication, or just those associated with specified services. The served user's ability to originate communications is unaffected by the CFU supplementary service. After the CFU service has been activated, communications are forwarded independent of the status of the served user.

As a service provider option, a subscription option can be provided to enable the served user to receive an indication that the CFU service has been activated. This indication shall be provided when the served user originates a communication if the CFU service has been activated for the served user's address and for the service requested for the communication.

The maximum number of diversions permitted for each communication is a service provider option. The service provider shall define the upper limit of diversions. When counting the number of diversions, all types of diversion are included.

Reference(s)

3GPP TS 24.604 [106].

15.5.3 Test purpose

1) To verify that the UE can request activation of Communication unconditional with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Communication Forwarding; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.5.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated a PDP context with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Related ICS/IXIT Statement(s)

Support for MTSI (Yes/No)

Support for initiating a session (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Support for Communication Diversion (Yes/No)

GAA XCAP authentication (Yes/No)

HTTP Digest XCAP authentication (Yes/No)

Test procedure

1) Communication Forwarding is activated on the UE so that the incoming call will be unconditionally forwarded to SIP URI "sip:user@domain.com".

2) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself, add a rule for communication forwarding unconditional to target "sip:user@domain.com" and finally activate the communication forwarding service.

3) Communication Forwarding is deactivated on the UE.

4) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself and deactivate the communication forwarding. The UE may also delete any rules for communication forwarding.

15.5.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme it supports:

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1).

- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute set as "true"

  - within <cp:ruleset> one <cp:rule> element for communication forwarding as follows:

    - <cp:conditions> element missing or empty as forwarding is supposed to be unconditional

    - <cp:actions> element containing <forward-to> element containing <target> element

      - value of target address to be "sip:user@domain.com"

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute being set "false"

15.6 Communication Deflection

15.6.1 Definition and applicability

Test to verify that the MT UE correctly performs MTSI Communication Deflection. This process is described in 3GPP TS 24.173 [65] and TS 24.604 [106]. The test case is applicable for IMS security or GIBA.

15.6.2 Conformance requirement

[TS 24.604, clause 4.2.1.6]:

The CD service enables the served user to respond to an incoming communication by requesting redirection of that communication to another user. The CD service can only be invoked before the connection is established by the served user, i.e. in response to the offered communication (before ringing), i.e. CD Immediate, or during the period that the served user is being informed of the communication (during ringing). The served user's ability to originate communications is unaffected by the CD supplementary service.

The maximum number of diversions permitted for each communication is a network provider option. The network provider shall define the upper limit of diversions. When counting the number of diversions, all types of diversion are included.

Reference(s)

3GPP TS 24.604 [106] clause 4.2.1

15.6.3 Test purpose

1) To verify that the UE correctly returns 302 when initiating MTSI Communication Deflection

15.6.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step. UE is configured to deflect incoming sessions so that the session should be diverted to "sip:user@company.com".

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

GIBA (Yes/No)

Support for MTSI (Yes/No)

Support for initiating a session (Yes/No)

Support for speech (Yes/No)

Support for Communication Diversion (Yes/No)

Test procedure

1) SS sends an INVITE request to the UE.

2) SS may receive 100 Trying from the UE.

3) SS receives 302 Moved Temporarily from the UE.

4) SS send an ACK to the UE

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with the first SDP offer.
2	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response.
3	→		302 Moved Temporarily	The UE responds to INVITE with 302 Moved Temporarily
4	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.

NOTE: The default messages contents in annex A are used with condition 'IMS security ' or 'GIBA' when applicable

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9, with the following exceptions:

Header/param	Value/Remark
Supported option-tag	*precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o= - 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=IMS conformance test* - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVPF 99* - *c= IN* (addrtype) (connection-address for SS) - *b=AS:30* Attributes for media: - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

100 Trying for INVITE (Step 2)

Use the default message '100 Trying for INVITE' in annex A.2.2

302 Moved Temporarily (Step 3)

Use the default message '302 Moved Temporarily' in annex A.4.5

ACK (Step 4)

Use the default message 'ACK' in annex A.2.7

15.6.5 Test requirements

The UE shall send requests and responses as described in clause 15.6.4

15.7 Communication Forwarding on non Reply: activation

15.7.1 Definition and applicability

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding for the case when user does not answer to the phone. This process is described in 3GPP TS 24.604 [106]. The test case is applicable for IMS security or GIBA.

15.7.2 Conformance requirement

Generic requirements for Communication Forwarding can be found from Annexes F1 and F.4..

[TS 24.604, clause 4.2.1.4]:

The CFNR service enables a served user to have the network redirect to another user communications which are addressed to the served user's address, and for which the connection is not established within a defined period of time. The CFNR service may operate on all communications, or just those associated with specified services. The served user's ability to originate communications is unaffected by the CFNR supplementary service.

The CFNR service can only be invoked by the network after the communication has been offered to the served user and an indication that the called user is being informed of the communication has been received.

As a service provider option, a subscription option can be provided to enable the served user to receive an indication that the CFNR service has been activated. This indication shall be provided when the served user originates a communication if the CFNR service has been activated for the served user's address and for the service requested for the communication.

The maximum number of diversions permitted for each communication is a service provider option. The service provider shall define the upper limit of diversions. When counting the number of diversions, all types of diversion are included.

Reference(s)

3GPP TS 24.604 [106]

15.7.3 Test purpose

1) To verify that the UE can request activation of Communication Forwarding (when the called user does not answer) with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Communication Forwarding; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.7.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated a PDP context with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Related ICS/IXIT Statement(s)

Support for MTSI (Yes/No)

Support for initiating a session (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Support for Communication Diversion (Yes/No)

Support for no reply timer setting (Yes/No)

GAA XCAP authentication (Yes/No)

HTTP Digest XCAP authentication (Yes/No)

Test procedure

1) Communication Forwarding is activated on the UE so that when the user does not answer, the incoming call will be forwarded to SIP URI "sip:user@domain.com". If the UE supports no reply timer setting, the value shall be set as 10 seconds.

2) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself, add a rule for communication forwarding due to no-answer to target "sip:user@domain.com" and finally activate the communication forwarding service.

3) Communication Forwarding is deactivated on the UE.

4) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself and deactivate the communication forwarding. The UE may also delete any rules for communication forwarding.

15.7.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports :

- HTTP Digest authentication

- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).-

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute set as "true"
  - within <cp:ruleset> one <cp:rule> element for communication forwarding as follows:
    - <cp:conditions> element containing a <no-answer> element
    - <cp:actions> element containing <forward-to> element containing <target> element. Additionally <NoReplyTimer> element shall be included, if the UE supports no reply timer setting.
      - value of target address to be "sip:user@domain.com"- value of NoReplyTimer (if included) to be 10 seconds

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute being set "false"

15.8 Communication Forwarding on non reply: MO call initiation

15.8.1 Definition and applicability

Test to verify that the MTSI MO UE correctly handles session setup where call is being forwarded due to no reply. This process is described in 3GPP TS 24.604 [106], clauses 4.2.1, 4.5.2.1 and A.1.3 and 3GPP TS 24.229 [10], clause 9.2.3. The test case is applicable for IMS security or GIBA.

15.8.2 Conformance requirement

[TS 24.604, clause 4.2.1.4]:

The CFNR service enables a served user to have the network redirect to another user communications which are addressed to the served user's address, and for which the connection is not established within a defined period of time. The CFNR service may operate on all communications, or just those associated with specified services. The served user's ability to originate communications is unaffected by the CFNR supplementary service.

The CFNR service can only be invoked by the network after the communication has been offered to the served user and an indication that the called user is being informed of the communication has been received.

[TS 24.604, clause 4.5.2.1]:

When communication diversion has occurred on the served user side and the network option "*Originating*" user receives notification that his communication has been diverted (forwarded or deflected)" is set to true, the originating UA may receive a 181 (Call is being forwarded) response according to the procedures described in 3GPP TS 24.229 .

The Information given by the History header could be displayed by the UA if it is a UE.

[TS 24.229, clause 9.2.3]:

Since the UE does not know that forking has occurred until a second provisional response arrives, the UE will request the radio/bearer resources as required by the first provisional response. For each subsequent provisional response that may be received, different alternative actions may be performed depending on the requirements in the SDP answer:

- the UE has sufficient radio/bearer resources to handle the media specified in the SDP of the subsequent provisional response, or

- the UE must request additional radio/bearer resources to accommodate the media specified in the SDP of the subsequent provisional response.

NOTE 1: When several forked responses are received, the resources requested by the UE is the "logical OR" of the resources indicated in the multiple responses to avoid allocation of unnecessary resources. The UE does not request more resources than proposed in the original INVITE request.

NOTE 2: When service-based local policy is applied, the UE receives the same authorization token for all forked requests/responses related to the same SIP session.

When an 199 (Early Dialog Terminated) response for the INVITE request is received for an early dialogue, the UE shall release reserved radio/bearer resources associated with that early dialogue.

When the first final 200 (OK) response for the INVITE request is received for one of the early dialogues, the UE proceeds to set up the SIP session using the radio/bearer resources required for this session. Upon the reception of the first final 200 (OK) response for the INVITE request, the UE shall release all unneeded radio/bearer resources.

GIBA:

NOTE 1: GIBA does not allow SIP requests to be protected using an IPsec security association because it does not perform a key agreement procedure.

Reference(s)

3GPP TS 24.604 [106], clauses 4.2.1 and 4.5.2.1; 3GPP TS 24.229 [10], clause 9.2.3

15.8.3 Test purpose

1) To verify that when initiating MO call the UE handles correctly the successive 180 and 181 provisional responses received during call setup.

15.8.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Related ICS/IXIT Statement(s)

- Support for initiating a session (Yes/No)
- Support for MTSI (Yes/No)
- Support for speech (Yes/No)
- Support for integration of resource management and SIP (use of preconditions) (Yes/No)
- Support for Communication Diversion (Yes/No)
- IMS security (Yes/No)
- GIBA (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-14) UE executes the procedures described in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 14 but only steps 1 to 11 of Annex C.21 in the parallel behaviour to steps 13-14 of table 4.5A.6.3-1.

15) SS responds to the INVITE with a valid 181 Call Is Being Forwarded response.

16) SS (now starting to simulate the UE to which call was forwarded) sends another 183 Session in Progress response to the INVITE request. As this response contains an SDP answer it is sent reliably.

17) SS waits for the UE to send a PRACK request, containing an SDP offer in which the UE tells to have reserved the local resources.

18) SS responds to the PRACK request with valid 200 OK response. The response contains an SDP answer which tells that SS has reserved its local resources as well.

19) SS responds to the INVITE request with 180 Ringing response.

20) SS responds to the INVITE request with valid 200 OK response.

21) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

22) Call is released on the UE. SS waits the UE to send a BYE request.

23) SS responds to the BYE request with valid 200 OK response.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-9B			Steps 1-11 as defined in Annex C.21	The same messages as in steps 2 - 11 of Annex C.21 are used. Referred from 36.508 [94] table 4.5A.6.3-1 for a UE with E-UTRA support.
10	←		181 Call is being forwarded	SS sends 181 response to indicate that call forwarding has been started as the user did not answer to the phone
11	←		183 Session Progress	SS (simulating the phone to which the call was forwarded) responds with 183 Session Progress containing an SDP answer indicating support for AMR codec and state of the local preconditions. UE will consider this response as forked one since it has different To tag this time compared to step 8.
12-13B			Steps 5-8 as defined in Annex C.21	The same messages as specified in steps 5 - 8 of Annex C.21 are used with To-tag and Contact Address as in the 183 response of step 11
14	←		180 Ringing	The SS sends 180 Ringing response to the UE
14A	→		PRACK	UE acknowledges the receipt of 180 response by sending PRACK.
14B	←		200 OK	The SS responds PRACK with 200 OK.
15	←		200 OK	The SS responds INVITE with 200 OK to indicate that the virtual remote UE had answered the call
16	→		ACK	The UE acknowledges the receipt of 200 OK for INVITE
17	→		BYE	The UE releases the call with BYE
18	←		200 OK	The SS sends 200 OK for BYE

NOTE: The default messages contents in annex A are used with condition 'IMS security' or 'GIBA' when applicable

Specific Message Contents

181 Call is being forwarded for INVITE (Step 10)

Use the default message '181 Call is being forwarded' in annex A.2.14

183 Session Progress for INVITE (Step 11)

Use the default message '183 Session in Progress for INVITE' in annex A.2.3 with the following exceptions:

Header/param	Value/remark
To	
tag	different tag must be used than the one used in steps 3-9 as this response is now from another UE and belongs to another dialog instance. Note that this new tag must be used within the rest of the steps (10-17) in this test case instead of the tag used within steps 3-9.
Contact	
addr-spec	different URI must be used than the one used in step 3 as this is supposed now to represent another UE to which the call is being forwarded. . Note that this new Contact must be used within the rest of the steps (13-14) in this test case.
Require	
option-tag	*precondition, 100rel*
Message-body	Same contents as specified in step 4 annex C.21.

180 Ringing for INVITE (Step 14)

Use the default message '180 Ringing for INVITE' in annex A.2.6 applying condition A3 (Response sent reliably) and with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	Same value as in the 183 response of step 11
History-Info	
hi-targeted-to-uri	Same value as in the 181 response of step 10
hi-index	Same value as in the 181 response of step 10

PRACK (Step 14A)

Use the default message 'PRACK' in annex A.2.4.

200 OK for PRACK (Step 14B)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

200 OK for INVITE (Step 15)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	Same value as in the 183 response of step 11
History-Info	
hi-targeted-to-uri	Same value as in the 181 response of step 10
hi-index	Same value as in the 181 response of step 10

ACK (Step 16)

Use the default message 'ACK' in annex A.2.7.

BYE (Step 17)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE (Step 18)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

15.8.5 Test requirements

SS must check that if the UE uses IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

15.9 Communication Forwarding on Busy

15.9.1 Definition and applicability

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding for the case when user is busy. This process is described in 3GPP TS 24.604 [106]. The test case is applicable for IMS security or GIBA.

15.9.2 Conformance requirement

Generic requirements for Communication Forwarding can be found from Annexes F.1 and F.4.

[TS 24.604, clause 4.2.1.3]:

The CFB service enables a served user to have the network redirect to another user communications which are addressed to the served user's address and meet busy. The CFB service may operate on all communications, or just those associated with specified services. The served user's ability to originate communications is unaffected by the CFB supplementary service.

As a service provider option, a subscription option can be provided to enable the served user to receive an indication that the CFB service has been activated. This indication shall be provided when the served user originates a communication if the CFB service has been activated for the served user's address and for the service requested for the communication.

The maximum number of diversions permitted for each communication is a service provider option. The service provider shall define the upper limit of diversions. When counting the number of diversions, all types of diversion are included.

Reference(s)

3GPP TS 24.604 [106]

15.9.3 Test purpose

1) To verify that the UE can request activation of Communication Forwarding (when the called user is busy) with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Communication Forwarding; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.9.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated a PDP context with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Related ICS/IXIT Statement(s)

Support for MTSI (Yes/No)

Support for initiating a session (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Support for Communication Diversion (Yes/No)

GAA XCAP authentication (Yes/No)

HTTP Digest XCAP authentication (Yes/No)

Test procedure

1) Communication Forwarding is activated on the UE so that when the user is busy, the incoming call will be forwarded to SIP URI "sip:user@domain.com".

2) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself, add a rule for communication forwarding due to busy to target "sip:user@domain.com" and finally activate the communication forwarding service.

3) Communication Forwarding is deactivated on the UE.

4) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself and deactivate the communication forwarding. The UE may also delete any rules for communication forwarding.

15.9.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports:

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1).

- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute set as "true"

  - within <cp:ruleset> one <cp:rule> element for communication forwarding as follows:

    - <cp:conditions> element containing a <busy> element

    - <cp:actions> element containing <forward-to> element containing <target> element

- value of target address to be "sip:user@domain.com"

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute being set "false"

15.10 Communication Forwarding on Not logged-in

15.10.1 Definition and applicability

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding for the case when user is not registered to IMS service. This process is described in 3GPP TS 24.604 [106]. The test case is applicable for IMS security or GIBA.

15.10.2 Conformance requirement

Generic requirements for Communication Forwarding can be found from Annexes F.1 and F.4.

[TS 24.604, clause 4.2.1.7]:

The Communication Forwarding on Not Logged-in (CFNL) service enables a served user to redirect incoming communications which are addressed to the served user's address, to another user (forwarded-to address) in case the served user is not registered (logged-in). The CFNL service may operate on all communications, or just those associated with specified basic services.

As a service provider option, a subscription option can be provided to enable the served user to receive an indication that the CFNL service has been activated. This indication shall be provided when the served user logs out according to procedures described in RFC 3261

The maximum number of diversions permitted for each communication is a service provider option. The service provider shall define the upper limit of diversions. When counting the number of diversions, all types of diversion are included.

Reference(s)

3GPP TS 24.604 [106]

15.10.3 Test purpose

1) To verify that the UE can request activation of Communication Forwarding (when the called user is not logged in) with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Communication Forwarding; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.10.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated a PDP context with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Related ICS/IXIT Statement(s)

Support for MTSI (Yes/No)

Support for initiating a session (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Support for Communication Diversion (Yes/No)

GAA XCAP authentication (Yes/No)

HTTP Digest XCAP authentication (Yes/No)

Test procedure

1) Communication Forwarding is activated on the UE so that when the user is not logged into IMS, the incoming call will be forwarded to SIP URI "sip:user@domain.com".

2) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself, add a rule for communication forwarding due to not-registered to target "sip:user@domain.com" and finally activate the communication forwarding service.

3) Communication Forwarding is deactivated on the UE.

4) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself and deactivate the communication forwarding. The UE may also delete any rules for communication forwarding.

15.10.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports:

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1).

- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute set as "true"

  - within <cp:ruleset> one <cp:rule> element for communication forwarding as follows:

    - <cp:conditions> element containing a <not-registered> element

    - <cp:actions> element containing <forward-to> element containing <target> element

      - value of target address to be "sip:user@domain.com"

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute being set "false"

15.10a Communication Forwarding on Not reachable

15.10a.1 Definition and applicability

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Forwarding for the case when user is not reachable. This process is described in 3GPP TS 24.604 [106]. The test case is applicable for IMS security or GIBA.

15.10a.2 Conformance requirement

Generic requirements for Communication Forwarding can be found from Annexes F.1 and F.4.

[TS 24.604]:

Communication Forwarding on Subscriber Not Reachable (CFNRc)

The CFNRc service enables an user to have the network redirect all incoming communications, when the user is not reachable (e.g. there is no IP connectivity to the user's terminal), to another user. The CFNRc service may operate on all communications, or just those associated with specified services. The user's ability to originate communications is unaffected by the CFNRc simulation service.

As a service provider option, a subscription option can be provided to enable the user to receive an indication that the CFNRc service has been activated. This indication may be provided when the user originates a communication if the CFNRc service has been activated for the user and for the service requested for the communication.

The maximum number of diversions permitted for each communication is a service provider option. The service provider shall define the upper limit of diversions. When counting the number of diversions, all types of diversion are included.

Reference(s)

3GPP TS 24.604 [106]

15.10a.3 Test purpose

1) To verify that the UE can request activation of Communication Forwarding (when the called user is not reachable) with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Communication Forwarding; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.10a.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated a PDP context with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Related ICS/IXIT Statement(s)

Support for MTSI (Yes/No)

Support for initiating a session (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Support for Communication Diversion (Yes/No)

GAA XCAP authentication (Yes/No)

HTTP Digest XCAP authentication (Yes/No)

Test procedure

1) Communication Forwarding is activated on the UE so that when the user is not reachable, the incoming call will be forwarded to SIP URI "sip:user@domain.com".

2) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself, add a rule for communication forwarding due to not-reachable to target "sip:user@domain.com" and finally activate the communication forwarding service.

3) Communication Forwarding is deactivated on the UE.

4) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself and deactivate the communication forwarding. The UE may also delete any rules for communication forwarding.

15.10a.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports:

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1).

- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute set as "true"

  - within <cp:ruleset> one <cp:rule> element for communication forwarding as follows:

    - <cp:conditions> element containing a <not-reachable> element

    - <cp:actions> element containing <forward-to> element containing <target> element

      - value of target address to be "sip:user@domain.com"

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <communication-diversion> element with "active" attribute being set "false".

15.11 MO Call Hold without announcement

15.11.1 Definition and applicability

Test to verify that the UE correctly performs IMS mobile originated call hold and resume. This process is described in 3GPP TS 24.610 [108], The test case is applicable for IMS security or GIBA.

15.11.2 Conformance requirement

[TS 24.610 clause 4.5.2.1]:

In addition to the application of procedures according to 3GPP TS 24.229, the following procedures shall be applied at the invoking UE in accordance with RFC 3264.

If individual media streams are affected, the invoking UE shall generate a new SDP offer where:

- for each media stream that is to be held, the SDP offer that contains:
  - an "inactive" SDP attribute if the stream was previously set to "recvonly" media stream; or
  - a "sendonly" SDP attribute if the stream was previously set to "sendrecv" media stream;
- for each media stream that is to be resumed, the SDP offer contains:
  - a "recvonly" SDP attribute if the stream was previously an inactive media stream; or
  - a "sendrecv" SDP attribute if the stream was previously a sendonly media stream, or the attribute may be omitted, since sendrecv is the default; or
- for each media stream that is unaffected, the media parameters in the SDP offer remain unchanged from the previous SDP offer.

If all the media streams are to be held, the invoking UE shall generate an SDP offer containing a session level direction attribute, or separate media level direction attributes, in the SDP that is set to:

- "inactive" if the streams were previously set to "recvonly" media streams; or
- "sendonly" if the streams were previously set to "sendrecv" media streams; or

If all the media streams that shall be resumed, the invoking UE shall generate a session level direction attribute, or separate media level direction attributes, in the SDP that is set to:

- "recvonly" if the streams were previously inactive media streams; or
- "sendrecv" if the streams were previously sendonly media streams, or the attribute may be omitted, since sendrecv is the default.

Then the UE shall send the generated SDP offer in a re-INVITE request (or UPDATE request) to the remote UE.

[TS 26.114 clause 7.3.1]:

RTCP packets should be sent for all types of multimedia sessions to enable synchronization with other RTP transported media, remote end-point aliveness information, monitoring of the transmission quality, and carriage of feedback messages such as TMMBR for video and RTCP APP for speech. Point-to-point speech only sessions may not require these functionalities and may therefore turn off RTCP by setting the SDP bandwidth modifiers (RR and RS) to zero. When RTCP is turned off (for point-to-point speech only sessions) and the media is put on hold, the MTSI client should re-negotiate the RTCP bandwidth with SDP bandwidth modifiers values greater than zero, and send RTCP packets to the other end. This allows the remote end to detect link aliveness during hold. When media is resumed, the resuming MTSI client should turn off the RTCP sending again through a re-negotiation of the RTCP bandwidth with SDP bandwidth modifiers equal to zero.

[TS 24.229 clause 6.1.1]:

If the media line in the SDP indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556, then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in subclause 6.1 of RFC 3890.

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in or 3GPP 29.213.

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifier will typically get the value of zero.

Reference(s)

3GPP TS 24.610 [108], 3GPP TS 24.229 [10]

15.11.3 Test purpose

1) To verify that the invoking UE puts the call to hold with a correct exchange of SIP/SDP protocol signalling messages; and

2) To verify that the invoking UE is able to resume the call with a correct exchange of SIP/SDP protocol signalling messages.

15.11.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF, registered to IMS services and set up the MO call, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step and thereafter executing the generic test procedure in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 14 for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1).

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and MO call.

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for MTSI (Yes/No)

Support for speech (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

Support for Communication Hold (Yes/No)

Support for sending RTCP while call is being hold (Yes/No)

Support for suppressing RTCP during the active two-way voice sessions (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Test procedure

1) Call hold is initiated on the UE. SS waits the UE to send an INVITE or UPDATE request with a SDP offer

2) If UE sent an INVITE request in step 1, SS responds to the it with a 100 Trying response. No such response is sent for UPDATE.

3) SS responds to the INVITE or UPDATE request with valid 200 OK response.

4) If UE sent an INVITE in step 1 SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

5) Call resume is initiated on the UE. SS waits the UE to send an INVITE or UPDATE request with a SDP offer

6) If UE sent an INVITE request in step 5, SS responds to it with a 100 Trying response. No such response is sent for UPDATE.

7) SS responds to the INVITE or UPDATE request with valid 200 OK response.

8) If UE sent an INVITE in step 5 SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

9) Call is released on the UE. SS waits the UE to send a BYE request.

10) SS responds to the BYE request with valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
			User initiates holding the call	
1-4			Steps specified in annex C.8 to hold the call	
			User initiates resuming the call	
5-8			Steps specified in annex C.8 to resume the call	
			User initiates releasing the call	
9	→		BYE	The UE releases the call with BYE
10	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

Messages in Step 1-4

Use messages according to annex C.8 to put the call to hold.

Messages in Step 5-8

Use messages according to annex C.8 to resume the call.

15.11.5 Test requirements

SS must check that if the UE uses IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

Step 1: the UE shall send an INVITE or UPDATE message with correct content. The UE shall include the same lines in the SDP body as specified for call hold in step 1 of annex C.8.

Step 5: the UE shall send an INVITE or UPDATE message containing an SDP message referred to step 3 of Annex C.8 to resume the call.

15.12 MT Call Hold without announcement

15.12.1 Definition and applicability

Test to verify that the UE correctly performs IMS mobile terminated call hold and resume. This process is described in 3GPP TS 24.610 [108]. The test case is applicable for IMS security or GIBA.

15.12.2 Conformance requirement

[TS 24.610 clause 4.5.2.9]:

Basic communication procedures according to TS 24.229 shall apply.

[TS 24.229 clause 6.1.1]:

If the media line in the SDP indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556, then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in subclause 6.1 of RFC 3890.

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in or 3GPP 29.213.

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent; therefore, the RR bandwidth modifier will typically get the value of zero.

[TS 26.114 clause 7.3.1]:

RTCP packets should be sent for all types of multimedia sessions to enable synchronization with other RTP transported media, remote end-point aliveness information, monitoring of the transmission quality, and carriage of feedback messages such as TMMBR for video and RTCP APP for speech. Point-to-point speech only sessions may not require these functionalities and may therefore turn off RTCP by setting the SDP bandwidth modifiers (RR and RS) to zero. When RTCP is turned off (for point-to-point speech only sessions) and the media is put on hold, the MTSI client should re-negotiate the RTCP bandwidth with SDP bandwidth modifiers values greater than zero, and send RTCP packets to the other end. This allows the remote end to detect link aliveness during hold. When media is resumed, the resuming MTSI client should turn off the RTCP sending again through a re-negotiation of the RTCP bandwidth with SDP bandwidth modifiers equal to zero.

Reference(s)

3GPP TS 24.610 [108], TS 24.229 [10]

15.12.3 Test purpose

1) To verify that the held UE responds correctly to call hold and resume requests from SS.

15.12.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF, registered to IMS services and set up the MO call, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step and thereafter executing the generic test procedure in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 14 for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1).

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and MO call.

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for MTSI (Yes/No)

Support for speech (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

Support for Communication Hold (Yes/No)

Support for sending RTCP while call is being hold (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Test procedure

1) SS initiates the call hold by sending a re-INVITE to set the media streams into sendonly state.
2) Optional: SS waits for the UE to respond to the INVITE request with a 100 Trying response.
3) SS waits for the UE to respond to the INVITE request with valid 200 OK response.
4) SS sends an ACK to acknowledge receipt of the 200 OK for INVITE.
5) SS resumes the call by sending another re-INVITE request with a SDP offer to set the media streams into sendrecv state again.
6) Optional: SS waits for the UE to respond to the INVITE request with a 100 Trying response.
7) SS waits for the UE to respond to the INVITE request with valid 200 OK response.
8) SS sends an ACK to acknowledge receipt of the 200 OK for INVITE.
9) SS sends a BYE request to the UE in order to release the call.
10) UE responds to the BYE request with valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with a SDP offer indicating all medias as sendonly
2	→		100 Trying	Optional: The UE responds with a 100 Trying provisional response
3	→		200 OK	The UE responds INVITE with 200 OK to indicate that the UE is no more expecting to receive any media
4	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE
5	←		INVITE	SS sends INVITE with a SDP offer indicating all medias as sendrecv
6	→		100 Trying	Optional: The UE responds with a 100 Trying provisional response
7	→		200 OK	The UE responds INVITE with 200 OK to indicate that the SS can again send media
8	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE
9	←		BYE	The SS releases the call with BYE
10	→		200 OK	The UE sends 200 OK for BYE

Specific Message Contents

INVITE (Step 1)

Use the default message 'INVITE for MT call setup' in annex A.2.9 with the following exceptions:

The SS shall include the same lines in the SDP body as finally accepted for the dialog but change the directionality of all media lines as "sendonly". Version number of the SDP must be incremented by one compared to the previous SDP sent by the SS.

100 Trying for INVITE (Step 2)

Use the default message '100 Trying for INVITE' in annex A.2.2.

200 OK for INVITE (Step 3)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Message-body	Properly generated SDP answer to the SDP offer contained in the INVITE including: - All mandatory SDP lines as specified in RFC 4566[27]. - The same number of media lines ('m=') as in the INVITE. - All the media lines having directionality as "recvonly - RTCP 'RR' and 'RS' modifiers having values greater than zero, if the UE supports sending RTCP while call is being hold"

ACK (Step 4)

Use the default message 'ACK' in annex A.2.7.

INVITE (Step 5)

Use the default message 'INVITE for MT call setup' in annex A.2.9 with the following exceptions:

The SS shall include the same lines in the SDP body as in Step 1 but change the directionality of all media lines as "sendrecv". Version number of the SDP must be incremented by one compared to the previous SDP sent by the SS.

100 Trying for INVITE (Step 6)

Use the default message '100 Trying for INVITE' in annex A.2.2.

200 OK for INVITE (Step 7)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Message-body	Properly generated SDP answer to the SDP offer contained in the INVITE including: - All mandatory SDP lines as specified in RFC 4566[27]. - The same number of media lines ('m=') as in the INVITE. - All the media lines having directionality as "sendrecv"

ACK (Step 8)

Use the default message 'ACK' in annex A.2.7.

BYE (Step 9)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE (Step 10)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

15.12.5 Test requirements

SS must check that the UE correctly responds to all the mid-dialog INVITEs sent by the SS.

15.13 Incoming Communication Barring except for a specific user

15.13.1 Definition and applicability

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Barring (CB) correctly when incoming calls are allowed from one single address only. This process is described in 3GPP TS 24.611 [101]. The test case is applicable for IMS security or GIBA.

15.13.2 Conformance requirement

Generic requirements for activating and deactivating Communication Barring can be found from Annexes F.1 and F.5 of this document. Summary of the XML conditions specific to this test case is given here:

[TS .24.611]:

cp:identity: This condition evaluates to true when the remote user's identity matches with the value of the identity element. The interpretation of all the elements of this condition is described in the in the common policy draft (see RFC 4745). In all other cases the condition evaluates to false.

...

ocp:other-identity: If present in any rule, the "other-identity" element, which is empty, matches all identities that are not referenced in any rule. It allows for specifying a default policy. The exact interpretation of this condition is specified in OMA-TS-XDM_Core.

Reference(s)

3GPP TS 24.611 [101].

15.13.3 Test purpose

1) To verify that the UE can request activation of Incoming Communication Barring with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Incoming Communication Barring; and

3) To verify that the UE supporting HTTP Digest authentication can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.13.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated a PDP context with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Related ICS/IXIT Statement(s)

Support for MTSI (Yes/No)

Support for initiating a session (Yes/No)

Support for Communication Barring (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

GAA XCAP authentication (Yes/No)

HTTP Digest XCAP authentication (Yes/No)

Test procedure

1) Incoming Communication Barring is activated on the UE so that all incoming calls will be barred except when the SIP URI of the caller is "sip:user@domain.com".

2) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself and add a rule for barring incoming communication from all other users except "sip:user@domain.com" and finally activate the incoming communication barring.

3) Incoming Communication Barring is deactivated on the UE.

4) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself and deactivate the incoming communication barring. The UE may also delete any rules for incoming communication barring.

15.13.5 Test requirements

1. SS shall check that the UE can authenticate itself with correctly with the authentication scheme that the UE supports:

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1).

- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

Option 1:

- <incoming-communication-barring> element with "active" attribute set as "true"

  - within <cp:ruleset> one <cp:rule> element for incoming communications barring as follows:

- <cp:conditions> element containing an <cp:identity> element containing a <cp:many> element
  - element <cp:except id="sip:user@domain com"> within the <cp:many> element
- <cp:actions> element containing <allow> element with value "false"

Option 2:

- <incoming-communication-barring> element with "active" attribute set as "true"
  - within <cp:ruleset> two rules as follows:
    - one <cp:rule> element for incoming communications barring as follows:
      - <cp:conditions> element containing an <cp:identity> element
        - element <cp:one id="sip:user@domain com"> within the <cp:identity> element
      - <cp:actions> element containing <allow> element with value "true"
    - another <cp:rule> element for incoming communications barring as follows:
      - <cp:conditions> element containing an empty <ocp:other-identity> element
      - <cp:actions> element containing <allow> element with value "false"

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <incoming-communication-barring> element with "active" attribute being set "false"

15.14 Incoming Communication Barring for anonymous users

15.14.1 Definition and applicability

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Barring (CB) correctly when incoming calls are rejected for anonymous users. This process is described in 3GPP TS 24.611 [101]. The test case is applicable for IMS security or GIBA.

15.14.2 Conformance requirement

Generic requirements for activating and deactivating Communication Barring can be found from Annexes F.1 and F.5 of this document. Summary of the XML conditions specific to this test case is given here:

[TS 24.611, clause 4.2.1]:

The Anonymous Communication Rejection (ACR) service allows the served user to reject incoming communications on which the asserted public user identity of the originating user is restricted. In case the asserted public user identity of the originating user is not provided then the communication shall be allowed by the ACR service.

An example where the originating user restricts presentation of the asserted public user identity is when he activated the OIR service 3GPP TS 24.607 .

The originating user is given an appropriate indication that the communication has been rejected due to the application of the ACR service.

The Anonymous Communication Rejection (ACR) simulation service is a special case of the ICB service, which is highlighted here because it is a regulatory service in many countries. The ACR service can be activated for a specific subscriber by configuring an ICB service barring rule where the conditional part contains the "Condition=anonymous" and the action part "allow=false".

[TS 24.611, clause 4.5.2.6.2]:

The AS providing the ACR service shall reject all incoming communications where the incoming SIP request:

1) includes the P-Asserted-Identity header field AND includes the Privacy header field indicating "id" as specified in RFC 3325; or

2) includes the P-Asserted-Identity header field AND includes the Privacy header field indicating "header" as specified in RFC 3323; or

3) includes the P-Asserted-Identity header field AND includes the Privacy header field indicating "user" as specified in RFC 3323; or

4) includes the P-Asserted-Identity header field AND includes the Privacy header field indicating "critical" as specified in RFC 3323.

[TS 24.611, clause 4.9.1.4]:

anonymous: To comply with the requirements as set for simulation of the ACR service, the *anonymous* element shall only evaluate to true when the conditions as set out in clause 4.5.2.6.2 for asserted originating public user identity apply.

Reference(s)

3GPP TS 24.611 [101], clauses 4.2.1, 4.5.2.6.2 and 4.9.1.4

15.14.3 Test purpose

1) To verify that the UE can request activation of Anonymous Communication Rejection with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Anonymous Communication Rejection; and

3) To verify that the UE supporting HTTP Digest authentication can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.14.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated a PDP context with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Related ICS/IXIT Statement(s)

Support for MTSI (Yes/No)

Support for initiating a session (Yes/No)

Support for anonymous communication rejection (ACR) (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

GAA XCAP authentication (Yes/No)

HTTP Digest XCAP authentication (Yes/No)

Test procedure

1) Anonymous Communication Rejection is activated on the UE

2) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself and add a rule for barring incoming communication from all anonymous users and finally activate the incoming communication barring.

3) Anonymous Communication Rejection is deactivated on the UE.

4) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself and deactivate the incoming communication barring. The UE may also delete any rules for incoming communication barring.

15.14.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports :

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1).
- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <incoming-communication-barring> element with "active" attribute set as "true"
  - within <cp:ruleset> one <cp:rule> element for incoming communications barring as follows:
    - <cp:conditions> element containing an <anonymous> element
    - <cp:actions> element containing <allow> element with value "false"

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <incoming-communication-barring> element with "active" attribute being set "false"

15.14a Communication Barring while roaming

15.14a.1 Definition and applicability

Test to verify that the UE activates and deactivates IMS Multimedia Telephony Communication Barring for incoming and outgoing calls while the user is roaming. This process is described in 3GPP TS 24.611 [101].

15.14a.2 Conformance requirement

Generic requirements for Communication Barring can be found from Annexes F.1 and F.5.

[TS 24.611, clause 4.9.1.4]:

roaming: This condition evaluates to true when the served user is registered from an access network other then the served users home network.

NOTE: Whether the served user is registered from another network then the served users home network can be determined from the P-Visited-Network-ID header field specified in IETF RFC 3455 [15] and the P-Access-Network-Info header field specified in IETF RFC 3455 [15] both are provided during the registration process, see 3GPP TS 24.229 [2], subclause 5.7.1.3.

Reference(s)

3GPP TS 24.611 [101]

15.14a.3 Test purpose

1) To verify that the UE can request activation of Communication Barring for incoming and outgoing calls while the user is roaming with a correctly composed HTTP PUT request; and

2) To verify that the UE can request deactivation of Communication Barring; and

3) To verify that the UE can authenticate its HTTP requests by including a correctly composed Authorization header with credentials of the user to the request. The UE may either include the Authorization header to its initial request or when sending the request again after receiving 401 response from SS.

15.14a.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is configured with the name of the XCAP root directory on the XCAP server and the user's directory name. If needed the UE is also configured with the HTTP Digest password to be used for XCAP. UE has activated a PDP context with SS.

SS is configured with the HTTP Digest password for XCAP or shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE.

If the UE uses GAA as XCAP authentication scheme, GAA bootstrapping exchange has been performed according to annex C.29.2.

Related ICS/IXIT Statement(s)

Support for MTSI (Yes/No)

Support for initiating a session (Yes/No)

IMS security (Yes/No)

Support for Communication Barring (Yes/No)

GAA XCAP authentication (Yes/No)

HTTP Digest XCAP authentication (Yes/No)

Test procedure

1) Communication Barring for incoming and outgoing calls are activated on the UE for the condition that the user is roaming.

2) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself, add a rules for barring communication while the user is roaming and finally activate the communication barring.

3) Communication Barring is deactivated on the UE.

4) UE and SS exchange a sequence of HTTP requests and responses. In this sequence UE may query the contents of the simservs document or selected parts of it. The UE shall authenticate itself and deactivate the communication barring. The UE may also delete any rules for communication barring.

15.14a.5 Test requirements

1. SS shall check that the UE can authenticate itself correctly with the authentication scheme that the UE supports:

- HTTP Digest authentication (see Annex C.29.1 step 2 NOTE 1).

- GAA based authentication as specified in TS 33.222 [121] and TS 24.109 [119] (see Annex C.29.2).

2. SS shall check that after Annex C.29.1 step 6 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <incoming-communication-barring> element with "active" attribute set as "true"
  - within <cp:ruleset> one <cp:rule> element for communication forwarding as follows:
    - <cp:conditions> element containing a <roaming> element
      - <cp:actions> element containing <allow> element with value "false"
- <outgoing-communication-barring> element with "active" attribute set as "true"
  - within <cp:ruleset> one <cp:rule> element for communication forwarding as follows:
    - <cp:conditions> element containing a <roaming> element
      - <cp:actions> element containing <allow> element with value "false"

3. SS shall check that after step 9 the simservs document stored in the SS contains the following pieces of information supplied by the UE:

- <incoming-communication-barring> and <outgoing-communication-barring> elements with "active" attribute being set "false" or those elements simply deleted

15.15 Subscription to the MWI event package

15.15.1 Definition and applicability

Test to verify that the UE is able to subscribe a MTSI message waiting notification and handle such notifications received after subscription. This process is described in 3GPP TS 24.229 [10] and TS 24.606 [107]. The test case is applicable for IMS security or GIBA.

15.15.2 Conformance requirement

[TS 24.606, clause 4.1]:

The Message Waiting Indication (MWI) service enables the network, upon the request of a controlling user to indicate to the receiving user, that there is at least one message waiting.

[TS 24.606, clause 4.6]:

The application/simple-message-summary MIME type used to provide Message Summary and Message Waiting Indication Information shall be coded as described in clause 5 of RFC 3842.

The coding of the message types in the message-context-class values shall follow the rules defined in the specifications listed in the "reference" column of table 1.

Table 1: Coding requirements

Value	Reference
voice-message	RFC 3458
video-message	RFC 3938
fax-message	RFC 3458
pager-message	RFC 3458
multimedia-message	RFC 3458
text-message	RFC 3458
none	RFC 3458

The coding of the additional information about deposited messages in the application/simple-message-summary MIME type body shall be in alignment with the rules defined in clause 25 of RFC 3261 for SIP extension-header (clause 3.5 of RFC 3842) and follow the rules defined in the specifications listed in the "reference" column of table 2.

Table 2: Additional information

Header	Description	Reference
To:	Indicates the subscriber's public user identity used by correspondent to deposit a message.	clause 3.6.3 of RFC 2822
From:	Indicates the correspondent's public user identity, if available.	clause 3.6.2 of RFC 2822
Subject:	Indicates the topic of the deposited message as provided by correspondent.	clause 3.6.5 of RFC 2822
Date:	Indicates the time and date information about message deposit.	clause 3.6.1 of RFC 2822
Priority:	Indicates the message priority as provided by correspondent.	RFC 2156
Message-ID:	Indicates a single unique message identity.	clause 3.6.4 of RFC 2822
Message-Context:	Indicates a type or context of message.	RFC 3458

[TS 24.606, clause 4.7.1]:

The MWI service is immediately activated after successful SUBSCRIBE request from the subscriber's UE, see clause 4.7.2.

The MWI service is deactivated after subscription expiry or after unsuccessful attempt to deliver a notification about message waiting.

[TS 24.606, clause 4.7.2.1]:

When the subscriber user agent intends to subscribe for status information changes of a message account, it shall generate a SUBSCRIBE request in accordance with RFC 3265 and RFC 3842 and in alignment with the procedures described in TS 24.229.

Depending on the service provisioning the UE will address the SUBSCRIBE request either to one of the subscriber's public user identities or to the public service identity of the message account (see clause 4.5.1).

The subscriber's UE shall implement the "application/simple-message-summary" content type as described in RFC 3842.

Reference(s)

3GPP TS 24.606 clause 4.1, 4.6, 4.7.1 and 4.7.2.1

15.15.3 Test purpose

1) To verify that when subscribing the message waiting indicator the MTSI UE performs correct exchange of SIP protocol signalling messages; and

2) After the receipt of the NOTIFY message, if the MS has a UI with the capability to notify the user of a Message Waiting Indication, the MS shall provide the appropriate user indication (which is to be described by the manufacturer) for the message waiting.

15.15.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) but the UE has not yet executed test procedure specified in annex C.14. If public service identity of the message account will be used in the test, that identity is configured to the phone. Otherwise the phone is expected to use the public identity of the user when subscribing to Message Waiting Indication package.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE (IMS security) and accepted the registration.

Related ICS/IXIT Statement(s)

Support for IMS Multimedia Telephony (Yes/No)

Support for Message Waiting Indication (Yes/No)

Support for UI capable of showing user notification for Message Waiting Indication (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Description of the user indication for the message waiting.

Test procedure

1) The UE sends a SUBSCRIBE request for Message Waiting Indication package
2) SS responds to the SUBSCRIBE request with a valid 200 OK response
3) SS sends UE a NOTIFY request for the subscribed Message Waiting Indication event package referring to no messages waiting.
4) SS waits for the UE to respond the NOTIFY with 200 OK response.
5) SS sends UE a NOTIFY request for the subscribed Message Waiting Indication event package containing one messages waiting.
6) SS waits for the UE to respond the NOTIFY with 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		SUBSCRIBE	UE subscribes to the Message Waiting Indication event package.
2	←		200 OK	The SS responds SUBSCRIBE with 200 OK
3	←		NOTIFY	The SS sends initial NOTIFY for Message Waiting Indication event package
4	→		200 OK	The UE responds the NOTIFY with 200 OK
5	←		NOTIFY	The SS sends another NOTIFY for Message Waiting Indication event package, now referring to one voice message waiting
6	→		200 OK	The UE responds the NOTIFY with 200 OK

NOTE: The default messages contents in annex A are used with condition 'IMS security ' or 'GIBA' when applicable

Specific Message Contents

SUBSCRIBE (Step 1)

Use the default message 'SUBSCRIBE for Message Waiting Indication package' in annex A.6.1

200 OK for SUBSCRIBE (Step 2)

Use the default message '200 OK for SUBSCRIBE' in annex A.1.5

NOTIFY (Step 3)

Use the default message 'NOTIFY for Message Waiting Indication package' in annex A.6.2

200 OK for NOTIFY (Step 4)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

NOTIFY (Step 5)

Use the default message 'NOTIFY for Message Waiting Indication package' in annex A.6.2 but with the following exceptions:

Header/param	Value/remark
Message-body	*Messages-Waiting: yes* *Message-Account:* **any IMPU within the set of IMPUs on ISIM** or **px_MessageAccountIdentity** as in From header *Voice-Message: 1/0 (0/0)* *To:* <**any IMPU within the set of IMPUs on ISIM**> *From: <user2_public1@home1.net>* *Subject: call me back!* *Message-ID: 27775334485@***px_MessageServerDomainName** *Message-Context: voice-message*

200 OK for NOTIFY (Step 6)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

15.15.5 Test requirements

The UE shall send requests and responses as described in clause 15.15.4

After step 5, if the UE has a UI with the capability to notify the user of a Message Waiting Indication, it shall indicate to the user the message waiting as per 'Description of the user indication for the message waiting'.

15.16 Void

15.17 Creating and leaving a conference

15.17.1 Definition and applicability

Test to verify that the UE is able to create an IMS MTSI voice conference to the conference focus using conference factory URI. This process is described in 3GPP TS 24.229 [10], TS 24.173 [65] and TS 24.147 [84]. The test case is applicable for IMS security or GIBA.

15.17.2 Conformance requirement

[TS 24.147, clause 5.3.1.3]:

A conference can be created by means of SIP, as described in subclause 5.3.1.3.2 or subclause 5.3.1.3.3.

NOTE: Additionally, creation of a conference can be provided by other means.

The conference participant shall make use of the procedures for session establishment as described in subclauses 5.1.2A and 5.1.3 of 3GPP TS 24.229 when creating conferences by means of SIP.

...

Upon a request to create a conference with a conference factory URI, the conference participant shall:

1) generate an initial INVITE request in accordance with subclause 5.1.3.1 of 3GPP TS 24.229; and

2) set the request URI of the INVITE request to the conference factory URI.

On receiving a 200 (OK) response to the INVITE request with the "isfocus" feature parameter indicated in Contact header, the conference participant shall store the content of the received Contact header as the conference URI. In addition to this, the conference participant may subscribe to the conference event package as described in RFC 4575 by using the stored conference URI.

NOTE 1: A conference participant can decide not to subscribe to the conference event package for conferences with a large number of attendees, due to, e.g. the signalling traffic caused by the notifications about users joining or leaving the conference.

NOTE 2: A conference can also be created with a conference URI. The procedures for this case at the conference participant are identical to those for joining a conference, as described in subclause 5.3.1.4.1. It is not assumed that the conference participant is aware that the conference gets created in this case.

NOTE 3: The UE can discover the conference factory URI from the Management Object as defined in 3GPP TS 24.166. Further discovery mechanisms for the conference factory URI are outside the scope of the present document.

...

GIBA:

NOTE 1: GIBA does not allow SIP requests to be protected using an IPsec security association because it does not perform a key agreement procedure.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.2A and 5.1.3, TS 24.173 [65], Annex G and TS 24.147 [84], clause 5.3.1.3.

15.17.3 Test purpose

1) To verify that when creating a conference with conference factory URI the UE performs correct exchange of SIP protocol signalling messages with the conference factory; and

2) To verify that within SIP signalling the UE performs the correct exchange of SDP messages for negotiating media and indicating preconditions for resource reservation (as described by 3GPP TS 24.229 [10], clause 6.1).

3) To verify the correct SIP message exchange if the UE optionally subscribes to the conference event package.

15.17.4 Method of test

Initial conditions

UE contains either SIM application (GIBA), ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for MTSI (Yes/No)

Support for speech (Yes/No)

Support for Conference (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Test procedure

1-7) UE creates the voice conference. The same procedure as in steps 1 - 7 of clause 12.12.4 (MO speech call with resource reservation) are used to create the conference into the conference focus and negotiate the media.

8) SS responds to the INVITE request with valid 200 OK response.

9) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

10) SS waits the UE to optionally subscribe to the conference event package with a SUBSCRIBE message

11) If UE sent SUBSCRIBE, SS responds to it with 200 OK response.

12) If UE sent SUBSCRIBE, SS sends a NOTIFY for the conference event package to the UE.

13) If SS sent a NOTIFY, SS waits the UE to respond the NOTIFY with 200 OK.

14) UE leaves the created conference. SS waits the UE to send a BYE request.

15) SS responds to the BYE request with valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-7			Messages in MO speech call test case (clause 12.12.4)	The same messages as in steps 1 - 7 of clause 12.12.4 are used
8	←		200 OK	The SS responds INVITE with 200 OK and gives the final conference URI within the response
9	→		ACK	The UE acknowledges the receipt of 200 OK for INVITE
10	→		SUBSCRIBE	Optional: UE subscribes the conference event
11	←		200 OK	Optional: SS responds to the subscription
12	←		NOTIFY	Optional: SS sends the initial state of the conference event to the UE
13	→		200 OK	Optional: UE responds to the NOTIFY
14	→		BYE	The UE leaves the conference with BYE
15	←		200 OK	The SS sends 200 OK for BYE

NOTE: The default messages contents in annex A are used with condition 'IMS security' or 'GIBA' when applicable

Specific Message Contents

The specific message contents for steps 1 - 7 is otherwise identical to what has been specified in test case 12.12, but with the additional exceptions to steps 1 and 3 as below:

INVITE (Step 1)

Header/param	Value/remark
Request-Line	
Request-URI	px_ConferenceFactoryUri
To	
addr-spec	px_ConferenceFactoryUri

183 Session in Progress for INVITE (Step 3)

Header/param	Value/remark
Contact	
addr-spec	px_TemporaryConferenceUri
feature-param	*isfocus*

200 OK for INVITE (Step 8)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Record-Route	
rec-route	Same value as in the 183 response
Contact	
addr-spec	px_FinalConferenceUri
feature-param	*isfocus*

ACK (Step 9)

Use the default message 'ACK' in annex A.2.7.

SUBSCRIBE (Step 10)

Use the default message 'SUBSCRIBE for conference event package' in annex A.5.1.

200 OK for SUBSCRIBE (Step 11)

Use the default message '200 OK for SUBSCRIBE' in annex A.5.2.

NOTIFY (Step 12)

Use the default message 'NOTIFY for conference event package' in annex A.5.3.

200 OK for NOTIFY (Step 13)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

BYE (Step 14)

Use the default message 'BYE' in annex A.2.8 but with the following exceptions:

Header/param	Value/remark
Request-Line	
Request-URI	px_FinalConferenceUri

200 OK for BYE (Step 15)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

15.17.5 Test requirements

SS must check that if the UE uses IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

Steps 1-7: See the Test requirements of test case 12.12.

Step 9: the UE shall send an ACK request with the correct content, according to common message definitions.

Step 10: the UE shall optionally send a SUBSCRIBE request with the correct content, according to common message definitions.

Step 13: the UE shall respond to the NOTIFY sent by the SS

15.18 Inviting user to conference by sending a REFER request to the user

15.18.1 Definition and applicability

Test to verify that the UE is able to invite an user to a conference by sending a REFER request directly to the invited user. This process is described in 3GPP TS 24.147 [84]. The test case is applicable for IMS security or GIBA.

15.18.2 Conformance requirement

[TS 24.147, clause 5.3.1.5.2]:

Upon generating a REFER request that is destined to a user in order to invite that user to a specific conference, the conference participant shall:

1) set the request URI of the REFER request to the address of the user who is invited to the conference;

2) set the Refer-To header of the REFER request to the conference URI of the conference that the other user shall be invited to, including the "method" URI parameter set to "INVITE" or omit the "method" parameter; and

NOTE: Other headers of the REFER request will be set in accordance with 3GPP TS 24.229

3) send the REFER request towards the user who is invited to the conference.

The UE may additionally include the Referred-By header to the REFER request and set it to the URI of the conference participant that is sending the REFER request.

Afterwards the UE shall treat incoming NOTIFY requests that are related to the previously sent REFER request in accordance with RFC 3515 and may indicate the received information to the user.

Reference(s)

3GPP TS 24.147[84], clause 5.3.1.5.2

15.18.3 Test purpose

1) To verify that the UE sends a correctly composed REFER request to invite a user to conference; and

2) To verify that the UE correctly processes the NOTIFYs from the invited user; and

3) To verify that the UE correctly processes the NOTIFYs for the conference event package if the UE has subscribed to those.

15.18.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF, registered to IMS services by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step and thereafter created a conference by executing the generic test procedure in Annex C.10 up to its last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and conference.

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for MTSI (Yes/No)

Support for speech (Yes/No)

Support for Conference (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Test procedure

1) UE invites a user to the conference created. SS waits the UE to send to the invited user a REFER request, which refers to the conference created.

2) SS responds to the REFER request with a valid 202 Accepted response.

3) SS sends an initial NOTIFY to tell that the invited user is trying to join the conference.

4) UE responds to the NOTIFY request with valid 200 OK response.

5) SS sends the final NOTIFY to tell that the invited user has successfully joined the conference.

6) UE responds to the NOTIFY request with a valid 200 OK response.

7) Optional: If UE subscribed the conference event package during the generic test procedure of Annex C.10, SS sends a NOTIFY for the conference event package to the UE to notify that the user joined the conference.

8) If SS sent a NOTIFY, SS waits the UE to respond the NOTIFY with 200 OK.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REFER	UE sends REFER to SS referring to the conference
2	←		202 Accepted	The SS responds with a 202 final response
3	←		NOTIFY	The SS sends initial NOTIFY for the implicit subscription created by the REFER request
4	→		200 OK	The UE responds the NOTIFY with 200 OK
5	←		NOTIFY	The SS sends a NOTIFY related to REFER request to confirm that the invited user was able to join the conference
6	→		200 OK	The UE responds the NOTIFY with 200 OK
7	←		NOTIFY	Optional: If the UE has subscribed the conference event package, the SS sends a NOTIFY for conference event package to inform that the invited user was able to join the conference
8	→		200 OK	Optional: The UE responds the NOTIFY with 200 OK

Specific Message Contents

REFER (Step 1)

Use the default message 'MO REFER' in annex A.2.10 with the following exceptions:

Header/param	Value/remark
Request-URI	SIP URI of the user invited to the conference
Refer-To	
addr-spec	px_FinalConferenceUri
To	
addr-spec	SIP URI of the user invited to the conference
tag	no tag given
Call-ID	
callid	value different to that received in INVITE message used to create the conference
CSeq	
value	must be present, value not checked

202 Accepted for REFER (Step 2)

Use the default message '202 Accepted' in annex A.3.3.

NOTIFY (Step 3)

Use the default message 'MT NOTIFY for refer package' in annex A.2.11 with the following exceptions:

Header/param	Value/remark
Message-body	*SIP/2.0 100 Trying*

200 OK for NOTIFY (Step 4)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

NOTIFY (Step 5)

Use the default message 'MT NOTIFY for refer package' in annex A.2.11 with the following exceptions:

Header/param	Value/remark
Subscription-State	
substate-value	*terminated*
expires	omitted from the request
reason	*noresource*
Message-body	*SIP/2.0 200 OK*

200 OK for NOTIFY (Step 6)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

NOTIFY (Step 7)

Use the default message 'NOTIFY for conference event package' in annex A.5.3 with the following exceptions:

Header/param	Value/remark
Message-body	*<?xml version="1.0" encoding="UTF-8"?>* *<conference-info xmlns="urn:ietf:params:xml:ns:conference-info">* *entity="***px_FinalConferenceUri***"* *state="partial"* *version="1"* *<users>* *<user entity="* **SIP URI of the invited user***">* *<endpoint entity="* **Contact URI of the invited user***">* *<status>connected</status>* *<joining-method>dialed-in</joining-method>* *<media id="1">* *<type>audio</type>* *<label>11223</label>* *<src-id>***random SSRC value***</src-id>* *<status>sendrecv</status>* *</media>* *</endpoint>* *</users>* *</conference-info>*

200 OK for NOTIFY (Step 8)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

15.18.5 Test requirements

SS must check that the UE sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

15.19 Inviting user to conference by sending a REFER request to the conference focus

15.19.1 Definition and applicability

Test to verify that the UE is able to invite an user to a conference by sending a REFER request to the conference focus. This process is described in 3GPP TS 24.147 [84]. The test case is applicable for IMS security or GIBA.

15.19.2 Conformance requirement

[TS 24.147, clause 5.3.1.5.3]:

Upon generating a REFER request that is destined to the conference focus in order to invite another user to a specific conference, the conference participant shall:

1) set the request URI of the REFER request to the conference URI to which the user is invited to;

2) set the Refer-To header of the REFER request to the SIP URI or tel URL of the user who is invited to the conference;

3) either include the "method" URI parameter with the value "INVITE" or omit the "method" parameter in the Refer-To header; and

NOTE: Other headers of the REFER request will be set in accordance with 3GPP TS 24.229.

4) send the REFER request towards the conference focus that is hosting the conference.

The UE may additionally include the Referred-By header to the REFER request and set it to the URI of the conference participant that is sending the REFER request.

In case of an active session the UE may additionally include the Replaces header in the header portion of the SIP URI of the Refer-to header of the REFER request. The included Replaces header shall refer to the active dialog that is replaced by the ad-hoc conference. The Replaces header shall comply with RFC 3891.

Afterwards the UE shall treat incoming NOTIFY requests that are related to the previously sent REFER request in accordance with RFC 3515 and may indicate the received information to the user.

Reference(s)

3GPP TS 24.147[84], clause 5.3.1.5.3

15.19.3 Test purpose

1) To verify that the UE sends a correctly composed REFER request to invite a user to conference; and

2) To verify that the UE correctly processes the NOTIFYs from the invited user; and

3) To verify that the UE correctly processes the NOTIFYs for the conference event package if the UE has subscribed to those.

15.19.4 Method of test

Same as 34.229-1 clause 15.18.4 except

Test procedure

1) UE invites a user to the conference created. SS waits the UE to send to the conference focus a REFER request, which refers to the user to be invited to the conference.

Specific Message Contents

REFER (Step 1)

Use the default message 'MO REFER' in annex A.2.10 with the following exceptions:

Header/param	Value/remark
Request-URI	px_FinalConferenceUri
Refer-To	
addr-spec	SIP URI of the user invited to the conference
To	
addr-spec	px_FinalConferenceUri
tag	no tag given
Call-ID	
callid	value different to that received in INVITE message used to create the conference
CSeq	
value	must be present, value not checked

15.19.5 Test requirements

SS must check that the UE sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

15.20 Void

15.21 Joining a conference after being invited to it

15.21.1 Definition and applicability

Test to verify that the UE is able to join a MTSI voice conference after being invited to it. This process is described in 3GPP TS 24.147 [84]. The test case is applicable for IMS security or GIBA.

15.21.2 Conformance requirement

[TS 24.147, clause 5.3.1.4.1]:

Upon generating an initial INVITE request to join a conference for which the conference URI is known to the conference participant, the conference participant shall:

1) set the request URI of the INVITE request to the conference URI; and

2) send the INVITE request towards the conferencing AS that is hosting the conference.

NOTE 1: The initial INVITE request is generated in accordance with 3GPP TS 24.229.

NOTE 2: The conference participants can get the conference URI as described in subclause 5.3.1.4.2. Other mechanisms can also be used by the conference participant to become aware of the conference URI, but they are out of scope of this specification..

On receiving a 200 (OK) response to the INVITE request with the "isfocus" feature parameter indicated in Contact header, the conference participant shall store the contents of the received Contact header as the conference URI. In addition to that, the conference participant may subscribe to the conference event package as described in RFC 4575 by using the stored conference URI.

NOTE 3: A conference participant can decide not to subscribe to the conference event package for conferences with a large number of attendees, due to the signalling traffic caused by the notifications about e.g. users joining or leaving the conference.

Upon receipt of an INVITE request that includes a Replaces header, the conference participant shall apply the procedures described in RFC 3891 to the INVITE request.

[TS 24.147, clause 5.3.1.4.2]:

Upon receipt of a REFER request that either includes a Refer-To header which includes the "method" uri parameter set to INVITE or does not include the "method" URI parameter, the conference participant shall:

1) handle the REFER request in accordance with RFC 3515;

2) perform the actions as described in subclause 5.3.1.4.1 for a user joining a conference; and

3) if the received REFER request included a Referred-By header, include the Referred-By header in accordance with RFC 3892 in the INVITE request that is sent for joining the conference.

Reference(s)

3GPP TS 24.147 [84], clauses 5.3.1.4.1 and 5.3.1.4.2

15.21.3 Test purpose

1) To verify that the UE correctly processes the REFER request which invites the user to join the conference; and

2) To verify that the UE issues correctly composed NOTIFYs to report its progress; and

3) To verify that the UE sets up a new dialog with conference focus by sending an INVITE request; and

4) To verify that the UE terminates the dialog with the conference focus when receiving a BYE request.

15.21.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for MTSI (Yes/No)

Support for speech (Yes/No)

Support for Conference (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Test procedure

1) SS sends to the UE a REFER request, which refers to the conference focus.

2) SS waits the UE to respond to the REFER request with a valid 202 Accepted response.

3) SS waits the UE to send an INVITE request to the conference focus

4) SS responds to the INVITE request with a 100 Trying response

5) SS waits the UE to send an initial NOTIFY to tell that it is trying to join the conference.

6) SS responds to the NOTIFY request with valid 200 OK response.

7) SS responds to the INVITE request with a 183 Session in Progress response

8) SS waits for the UE to send a PRACK request possibly containing the second SDP offer.

9) SS responds to the PRACK request with valid 200 OK response.

10) SS waits for the UE to optionally send a UPDATE request containing the final SDP offer. UE will not send the UPDATE request if the PRACK in step 8 already contained the final offer with preconditions met.

11) SS responds to the UPDATE request (if UE sent one) with valid 200 OK response.

12) SS responds to the INVITE request with a 200 OK response

13) SS waits the UE to send an ACK and NOTIFY requests. Additionally the UE may send a SUBCRIBE request for the conference event package. The UE is allowed to send these requests in any order.

14) SS responds to the NOTIFY request with a valid 200 OK response.

15) If UE sent SUBSCRIBE, SS responds to it with 200 OK response.

16) If UE sent SUBSCRIBE, SS sends a NOTIFY for the conference event package to the UE.

17) If SS sent a NOTIFY, SS waits the UE to respond the NOTIFY with 200 OK.

18) SS sends a BYE request in order to remove the UE from the conference

19) SS waits the UE to respond to the BYE request with a valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		REFER	SS sends REFER to UE referring to the conference
2	→		202 Accepted	UE responds with a 202 Accepted response
3	→		INVITE	UE sends INVITE to set up a dialog with conference focus. UE indicates the medias and codecs the UE supports.
4	←		100 Trying	SS responds the INVITE with 100 Trying
5	→		NOTIFY	UE sends initial NOTIFY for the implicit subscription created by the REFER request
6	←		200 OK	SS responds the NOTIFY with 200 OK
7	←		183 Session in Progress	SS responds with an SDP answer only supporting AMR audio codec
8	→		PRACK	UE acknowledges the receipt of 183 response with PRACK and optionally offers second SDP that indicates preconditions as met
9	←		200 OK	The SS responds PRACK with 200 OK and answers the second SDP with mirroring its contents and indicates having reserved the resources if UE has also done so.
10	→		UPDATE	Optional step: UE sends an UPDATE after having reserved the resources with GPRS procedures for PDP context used for the media
11	←		200 OK	Optional step : The SS responds UPDATE with 200 OK and indicates having reserved the resources
12	←		200 OK	SS responds the INVITE with 200 OK
13	→		ACK NOTIFY SUBSCRIBE (optional message)	UE sends the ACK to complete three-way handshake for INVITE and NOTIFY to confirm that the UE was able to join the conference. Additionally the UE may subscribe to the conference event package related to the conference to which the user joined. Note that the UE may send these messages in any order
14	←		200 OK	SS responds the NOTIFY with 200 OK
15	←		200 OK	Optional step: SS responds to the subscription if the UE sent the SUBSCRIBE request
16	←		NOTIFY	Optional step: SS sends the initial state of the conference event to the UE if the UE subscribed it
17	→		200 OK	Optional step: UE responds to the NOTIFY
18	←		BYE	SS sends a BYE to remove the UE from the conference
19	→		200 OK	UE responds the BYE with 200 OK

In addition to the steps shown above the UE might send extra NOTIFY requests to indicate the progress e.g. after receiving the 183 response from the SS. As the timing of these optional NOTIFY requests from the UE is not deterministic, they are not shown in the expected sequence. SS must be prepared to receive such NOTIFY requests between steps 3 and 13 and respond to them with 200 OK response.

Specific Message Contents

REFER (Step 1)

Use the default message 'MT REFER' in annex A.2.12 with the following exceptions:

Header/param	Value/remark
Request-URI	Contact URI of the UE invited to the conference (as within the REGISTER request from the UE)
Refer-To	
addr-spec	px_FinalConferenceUri
Referred-by	-- check this
addr-spec	*sip:master@conference.com*
To	
addr-spec	SIP URI of the user invited to the conference
tag	no tag given
Call-ID	
callid	any value according to Call-ID syntax can be used
CSeq	
value	any value according to CSeq syntax can be used

202 Accepted for REFER (Step 2)

Use the default message '202 Accepted' in annex A.3.3.

INVITE (Step 3)

Use the default message 'INVITE for MO call setup' in annex A.2.1 with the following exceptions:

Header/param	Value/remark
Request-Line	
Request-URI	px_FinalConferenceUri
To	
addr-spec	px_FinalConferenceUri
Referred-by	
addr-spec	*sip:master@conference.com*
Supported	
option-tag	*100rel, precondition*

For the contents of the SDP body see test requirement details.

100 Trying for INVITE (Step 4)

Use the default message '100 Trying for INVITE' in annex A.2.2.

NOTIFY (Step 5)

Use the default message 'MO NOTIFY for refer package' in annex A.2.13 with the following exceptions:

Header/param	Value/remark
Message-body	*SIP/2.0 100 Trying*

200 OK for NOTIFY (Step 6)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

183 Session in Progress for INVITE (Step 7)

Use the default message '183 Session in Progress for INVITE' in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Require option-tag	*precondition*
Contact	
addr-spec	px_FinalConferenceUri
Message-body	SDP body of the 183 response copied from the received INVITE but modified as follows: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; and - For speech media, the SS shall indicate only ARM codec to be supported. For all other media lines SS shall set the port number as zero in order to reject non-speech streams. - the "a=" lines describing the current and desired state of the preconditions, updated as follows: a=curr:qos local [none or sendrecv] (* a=curr:qos remote [none or sendrecv] (* a=des:qos mandatory local sendrecv a=des:qos mandatory remote sendrecv a=conf:qos remote sendrecv *) The value of these direction-tags in 183 must be none if the UE has not yet reserved its resources, but otherwise sendrecv

PRACK (Step 8)

Use the default message 'PRACK' in annex A.2.4 with the exception that either Supported or Require header shall contain the "precondition" tag.

For the contents of the optional SDP body see test requirement details.

200 OK for PRACK (Step 9)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	header shall be present only if there is SDP in message-body *application/sdp*
Content-Length value	 length of message-body
Message-body	SDP body of the 200 response copied from the received PRACK, if it contained one but otherwise omitted. The copied SDP body must be modified as follows for the 200 OK response: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; and - For speech media, the SS shall indicate only ARM codec to be supported. For all other media lines SS shall set the port number as zero in order to reject non-speech streams. - the "a=" lines describing the current and desired state of the preconditions, as described in RFC 3312 [31], updated as follows: a=curr:qos local sendrecv a=curr:qos remote sendrecv a=des:qos mandatory local sendrecv a=des:qos mandatory remote sendrecv

UPDATE (Step 10) optional step used when PRACK contained a=curr:qos local none

Use the default message 'UPDATE' in annex A.2.5 with the exception that either Supported or Require header shall contain the "precondition" tag.

For the contents of the SDP body see test requirement details.

200 OK for UPDATE (Step 11) - optional step used when UE sent UPDATE

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type	
media-type	*application/sdp*
Content-Length	
value	length of message-body
Message-body	SDP body of the 200 response copied from the received UPDATE but modified as follows: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; and - For speech media, the SS shall indicate only ARM codec to be supported. For all other media lines SS shall set the port number as zero in order to reject non-speech streams. - the "a=" lines describing the current and desired state of the preconditions, as described in RFC 3312 [31], updated as follows: a=curr:qos local sendrecv a=curr:qos remote sendrecv a=des:qos mandatory local sendrecv a=des:qos mandatory remote sendrecv

200 OK for INVITE (Step 12)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	px_FinalConferenceUri

ACK (Step 13)

Use the default message 'ACK' in annex A.2.7.

NOTIFY (Step 13)

Use the default message 'MO NOTIFY for refer package' in annex A.2.13 with the following exceptions:

Header/param	Value/remark
Subscription-State	
substate-value	*terminated*
expires	omitted from the request
reason	*noresource*
Message-body	*SIP/2.0 200 OK*

SUBSCRIBE (Step 13)

Use the default message 'SUBSCRIBE for conference event package' in annex A.5.1.

200 OK for NOTIFY (Step 14)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

200 OK for SUBSCRIBE (Step 15)

Use the default message '200 OK for SUBSCRIBE' in annex A.5.2.

NOTIFY (Step 16)

Use the default message 'NOTIFY for conference event package' in annex A.5.3.

200 OK for NOTIFY (Step 17)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

BYE (Step 18)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE (Step 19)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

15.21.5 Test requirements

SS must check that the UE sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

Step 3: the UE shall send an INVITE message with correct content. The UE shall include the following lines in the SDP body:

- All mandatory SDP lines, as specified in SDP grammar in RFC 4566 [27] appendix A, including:
  - "o=" line indicating e.g. the session identifier and the IP address of the UE;
  - "c=" line indicating the IP address of the UE for receiving the media flow;
- Media description lines for the speech media proposed by UE for the transferred call. For the speech media at least the following lines must exist within the SDP:
  - "m=" line describing the media type as audio, transport port and protocol used for media and media format as RTP/AVP;
  - "b=" line proposing the application specific maximum bandwidth ("AS" modifier) for the media;
  - extra "a=" line for rtpmap attribute per each dynamic payload type given in the "m=" line. The UE shall offer at least the mandatory AMR codec;
  - "a=" line for fmtp attribute per each rtpmap attribute. The fmtp attribute must cover at least the following parameters defined in RFC 4867 [67] for the AMR codec:
    mode-change-capability with value 2
    max-red with a value between 0 and 65535
  - an a=sendrecv line
  - four "a=" lines describing the current and desired state of the preconditions, as described in RFC 3312 [31]. At this stage of the call setup the lines shall be as follows:
    a=curr:qos local [none or sendrecv]

a=curr:qos remote none
a=des:qos mandatory local sendrecv
a=des:qos optional remote sendrecv
These four "a=" lines may appear in any order.

...

Step 8: the UE shall send a PRACK request with the correct content. The UE may include a SDP body in the PRACK request if it did not indicate to have met preconditions already when sending the INVITE request. In that case the following lines shall be included in the SDP body of PRACK:

- All mandatory SDP lines are present; and
- "o" line shall be the same like in INVITE request, except that the version number shall be increased; and
- SDP must contain at least as many media description lines as the SDP in the INVITE contained. One of them must be for speech media with AMR codec supported by the SS; and
- four "a=" lines describing the current and desired state of the preconditions, as described in RFC 3312 [31]. At this stage of the call setup the lines shall be as follows:
  a=curr:qos local sendrecv
  a=curr:qos remote none
  a=des:qos mandatory local sendrecv
  a=des:qos optional remote sendrecv
  These four "a=" lines may appear in any order.
- as the UE has met its local preconditions the a=inactive line must be replaced with a=sendrecv line.

...

Step 10: the UE may conditionally send an UPDATE request with the correct content. The UE shall include the following lines in the SDP body:

- All mandatory SDP lines are present; and
- "o" line like in INVITE request, except that the version number shall be increased compared to the previously sent SDP offer; and
- SDP must contain at least as many media description lines as the SDP in the INVITE contained. One of them must be for speech media with AMR codec supported by the SS; and
- four "a=" lines describing the current and desired state of the preconditions, as described in RFC 3312 [31]. At this stage of the call setup the lines shall be as follows:
  a=curr:qos local sendrecv
  a=curr:qos remote none
  a=des:qos mandatory local sendrecv
  a=des:qos optional remote sendrecv
  These four "a=" lines may appear in any order.
- as the UE has met its local preconditions the a=inactive line must be replaced with a=sendrecv line.

15.21a Three way session creation

15.21a.1 Definition and applicability

Test to verify that the UE support Three Way Session creation. This process is described in Section 5.3.1.3.3 of 3GPP TS 24.147 [84], The test case is applicable for IMS security or early IMS security.

15.21a.2 Conformance requirement

[TS 24.147 clause 5.3.1.3.3]:

When a user is participating in two or more SIP sessions and wants to join together two of these active sessions to a so-called three-way session, the user shall perform the following steps.

1) create a conference at the conference focus by sending an INVITE request with the conference factory URI for the three-way session towards the conference focus, as described in subclause 5.3.1.3.2;

2) decide and perform for each of the active sessions that are requested to be joined to the three-way session, how the remote user shall be invited to the three-way session, which can either be:

   a) by performing the procedures for inviting a user to a conference by sending an REFER request to the user, as described in subclause 5.3.1.5.2; or

   b) by performing the procedures for inviting a user to a conference by sending a REFER request to the conference focus, as described in subclause 5.3.1.5.3;

3) release the active session with the user, by applying the procedures for session release in accordance with RFC 3261 [7], provided that a BYE request has not already been received, after a NOTIFY request has been received, indicating that the user has successfully joined the three-way session, i.e. including:

   a) a body of content-type "message/sipfrag" that indicates a "200 OK" response; and,

   b) a Subscription-State header set to the value "terminated"; and,

4) treat the created three-way session as a normal conference, i.e. the conference participant shall apply the applicable procedures of subclause 5.3.1 for it.

Reference(s)

3GPP TS 24.147 [84]

15.21a.3 Test purpose

1) To verify that the invoking UE is able to create a three-way session by sending a REFER request to the conference focus to inviting a user to a conference;

15.21a.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF, registered to IMS services and set up the MO call, by executing the generic test procedure in Annex C.2 or C.2a (early IMS security only) up to the last step and thereafter executing the generic test procedure in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 14 for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1).

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and MO call.

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for MTSI (Yes/No)

Support for speech (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

Support for Communication Hold (Yes/No)

Support for sending RTCP while call is being hold (Yes/No)

Support for suppressing RTCP during the active two-way voice sessions (Yes/No)

Support for Conference (Yes/No)

Support for Three Way Session Creation (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-4) Call hold is initiated on the UE. The same steps defined in Annex C.8 are used to put the call into hold.

5-17) A new session is created by using the steps defined in Annex C.21.

18-30) UE initiates the conference creation process by executing the generic test procedure in Annex C.10.

31-38) UE invites one of the user who have session with the UE to the conference by performing the same procedure as in Annex C.19.

39-46) UE invites another user who have session with the UE to the conference by performing the same procedure as in Annex C.19.

UE shall send a BYE to terminate its session with SS. However timing of sending the BYE request is not fixedly defined and it may appear any time after step 46.

SS responds to the BYE request with a valid 200 OK response.

47) Optional: SS sends a BYE request to the UE in order to release the active session if BYE request has not already been received.

48) UE responds to the BYE request with valid 200 OK response.

NOTE: Timing of BYE is not shown in the test sequence as it might appear to the SS between any of the messages 5 and 46 or after the message46. SS shall be prepared to respond the BYE immediately after receiving it from the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-4			Messages in Annex C.8	The same messages as in Annex C.8 Steps 1-4 are used.
5-17			Steps defined in Annex C.21	The same messages as in Annex C.21 are used.
18-30			Steps defined in Annex C.10	The same messages as in Annex C.10 are used.
31-38			Steps defined in Annex C.19	The same messages as in Annex C.19 steps 1-8 are used.
39-46	→		Steps defined in Annex C.19	The same messages as in Annex C.19 steps 1-8 are used.
	→		BYE	UE shall send a BYE to terminate its session with SS. However timing of sending the BYE request is not fixedly defined and it may appear any time after step 46.
	←		200 OK	The SS responds the received BYE with 200 OK
47	←		BYE	Optional: The SS releases the active session with BYE
48	→		200 OK	The UE sends 200 OK for BYE

Specific Message Contents

INVITE(Step 6)

Header/param	Value/remark
Request-Line	
Request-URI	px_CalleeUri_Second px_CalleeUri_Second is used to invite another user to the session. px_ px_CalleeUri_Second may be either SIP or Tel URI. It may contain a dialstring and phone-context parameter, when calling to dialstring. When calling to dialstring SIP URI must also contain user=phone or user=dialstring parameter. The dialstring, if used, may be global, home local number or geo-local number. For home local numbers the value of phone-context parameter must equal the home domain name i.e. px_HomeDomainName. For geo-local numbers the home domain name must be prefixed by string 'geo-local.' or access technology specific prefix, if the UE supports that option. Note: The way how the UE determines whether numbers in a non-international format are geo-local, home-local or relating to another network, is UE implementation specific. For instance the UE might have a UI setting.
To	
addr-spec	px_CalleeUri_Second

BYE (Step 47)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE (Step 48)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

15.21a.5 Test requirements

SS must check that if the UE uses IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

The UE shall send requests and responses as described in clause 15.21a.4.

15.22 Void

15.23 MO Explicit Communication Transfer - Blind Call Transfer

15.23.1 Definition and applicability

Test to verify that the transferor UE correctly performs IMS Multimedia Telephony Explicit Communication Transfer (ECT) without consulting the transfer target prior to the transfer. This process is described in 3GPP TS 24.629 [104], Annex H. The test case is applicable for IMS security or GIBA.

15.23.2 Conformance requirement

[TS 24.629, clause 4.5.2.1]:

A UE that initiates a transfer operation, shall:

- Issue a REFER request in the original communications dialog, where:
  - The request URI shall contain the SIP URI of the transferee as received in the Contact header field.

- The Refer-To header field shall indicate the public address of the transfer Target.
- If the transferor UE has a (consultation) communication with the transfer Target, a Replaces header field parameter shall be added to the Refer-To URI together with a Require=replaces header field parameter.
- The Referred-By header field can be used to indicate the identity of the transferor. When privacy was required in the original communications dialog and a Referred-By header field is included, the UE shall include a Privacy header field set to "user".

After the REFER request is accepted by the other end with a 202 (Accepted) response, the transferor UE should get notifications of how the transferee's communication setup towards the transfer Target is progressing.

When a NOTIFY request is received on the REFER dialog that indicates that the transferee and the transfer Target have successfully setup a communication, the transferor UE may terminate the original communication with the transferee UE, by sending a BYE message on the original dialog.

Reference(s)

3GPP TS 24.629, clause 4.5.2.1 [104]

15.23.3 Test purpose

1) To verify that the transferor UE puts the call to hold before the transfer with a correct exchange of SIP/SDP protocol signalling messages; and
2) To verify that the transferor UE issues a correctly composed REFER request to initiate the call transfer; and
3) To verify that the transferor UE correctly processes the NOTIFYs from the transferee; and
4) To verify that the transferor UE terminates the dialog with the transferee with a BYE request.

15.23.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF, registered to IMS services and set up the MO call, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step and thereafter executing the generic test procedure in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 14 for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1). SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and MO call.

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for MTSI (Yes/No)

Support for speech (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

Support for Explicit Communication Transfer - blind transfer (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Test procedure

1-4) Call transfer is initiated on the UE. Steps defined in Annex C.8 are used to put the call into hold.

5) SS waits the UE to send a REFER request, which refers to the transfer target.

6) SS responds to the REFER request with a valid 202 Accepted response.

7) SS sends an initial NOTIFY to tell that the implicit refer subscription is pending.

8) UE responds to the NOTIFY request with valid 200 OK response.

9) SS sends the final NOTIFY to tell that the call transfer was successfully completed.

10) UE responds to the NOTIFY request with a valid 200 OK response.

11) UE shall send a BYE to terminate its session with SS. However timing of sending the BYE request is not fixedly defined and it may appear any time after step 5.

12) SS responds to the BYE request with a valid 200 OK response.

NOTE: Timing of BYE is not shown in the test sequence as it might appear to the SS between any of the messages 5 and 10 or after the message 10. SS shall be prepared to respond the BYE immediately after receiving it from the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-4			Steps defined in Annex C.8	The same messages as in steps 1 - 4 of Annex C.8 are used
5	→		REFER	UE sends REFER to SS referring to the transfer target
6	←		202 Accepted	The SS responds with a 202 final response
7	←		NOTIFY	The SS sends initial NOTIFY for the implicit subscription created by the REFER request
8	→		200 OK	The UE responds the NOTIFY with 200 OK
9	←		NOTIFY	The SS sends a NOTIFY to confirm that the call transfer has been completed
10	→		200 OK	The UE responds the NOTIFY with 200 OK
11	→		BYE	UE shall send a BYE to terminate its session with SS. However timing of sending the BYE request is not fixedly defined and it may appear any time after step 5.
12	←		200 OK	The SS responds the received BYE with 200 OK

Specific Message Contents

REFER (Step 5)

Use the default message 'MO REFER' in annex A.2.10

202 Accepted for REFER (Step 6)

Use the default message '202 Accepted' in annex A.3.3.

NOTIFY (Step 7)

Use the default message 'MT NOTIFY for refer package' in annex A.2.11 with the following exceptions:

Header/param	Value/remark
Message-body	*SIP/2.0 100 Trying*

200 OK for NOTIFY (Step 8)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

NOTIFY (Step 9)

Use the default message 'MT NOTIFY for refer package' in annex A.2.11 with the following exceptions:

Header/param	Value/remark
Subscription-State	
substate-value	*terminated*
expires	omitted from the request
reason	*noresource*
Message-body	*SIP/2.0 200 OK*

200 OK for NOTIFY (Step 10)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

BYE(step 11)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE(step 12)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

15.23.5 Test requirements

SS must check that the UE sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

SS must check that the UE sends a BYE to terminate its session with the SS at some point during the session transfer.

15.24 MT Explicit Communication Transfer - Blind Call Transfer

15.24.1 Definition and applicability

Test to verify that the transferee UE correctly performs IMS Multimedia Telephony Explicit Communication Transfer (ECT). This process is described in 3GPP TS 24.629 [104]. The test case is applicable for IMS security or GIBA.

15.24.2 Conformance requirement

When a REFER request is received in the context of a call transfer scenario (see clause 4.5.2.4.1), the transferee UE shall perform the following steps:

1) apply the procedure for holding the active communication with the transferor as described in 3GPP TS 24.610 clause 4.5.2.1; and

2) apply normal REFER handling procedures according to 3GPP TS 24.229 .

Reference(s)

3GPP TS 24.629, clause 4.5.2.1 [104]

15.24.3 Test purpose

1) To verify that the transferee UE is able to put the call to hold before the transfer with a correct exchange of SIP/SDP protocol signalling messages; and

2) To verify that the transferee UE correctly processes the REFER request which initiates the call transfer; and

3) To verify that the transferee UE issues a correctly composed NOTIFYs to the transferor; and

4) To verify that the transferee UE sets up a new dialog with transfer target by sending an INVITE request; and

5) To verify that the transferee UE terminates the dialog with the transferor when receiving a BYE request.

15.24.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF, registered to IMS services and set up a MO call by executing test case 12.12 (MO MTSI Voice Call Successful with preconditions) up to the step 12.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and the MO call.

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for MTSI (Yes/No)

Support for speech (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

Support for Explicit Communication Transfer - blind transfer (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Test procedure

1-4) The same procedure as in steps 1 - 4 of subclause 15.12.4 (MT Call hold) are used to put the call into hold.

5) SS sends to the UE a REFER request, which refers to the transfer target.

6) SS waits the UE to respond to the REFER request with a valid 202 Accepted response.

7) SS waits the UE to send an initial NOTIFY to tell that the implicit refer subscription is pending.

8) SS responds to the NOTIFY request with valid 200 OK response.

9) SS waits the UE to send an INVITE request to the transfer target

10) SS responds to the INVITE request with a 100 Trying response

11) SS responds to the INVITE request with 180 Ringing response.

12) SS waits for the UE to send a PRACK request.

13) SS responds to the PRACK request with valid 200 OK response.

14) SS responds to the INVITE request with a 200 OK response

15) SS waits the UE to send an ACK

16) SS waits the UE to send the final NOTIFY to tell that the call transfer was successfully completed.

17) SS responds to the NOTIFY request with a valid 200 OK response.

18) SS sends a BYE request in order to terminate its session with the UE

19) SS waits the UE to respond to the BYE request with a valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-4			Messages in MT Call Hold test case (subclause 15.12)	The same messages as in steps 1 - 4 of subclause 15.12.4 are used
5	←		REFER	SS sends REFER to SS referring to the transfer target
6	→		202 Accepted	UE responds with a 202 Accepted response
7	→		NOTIFY	UE sends initial NOTIFY for the implicit subscription created by the REFER request
8	←		200 OK	SS responds the NOTIFY with 200 OK
9	→		INVITE	UE sends INVITE to set up a dialog with transfer target. UE indicates the medias and codecs the UE supports. The UE has also reserved its resources.
10	←		100 Trying	SS responds the INVITE with 100 Trying
11	←		180 Ringing	The SS responds INVITE with 180 Ringing with SDP answer indicating that the resources have been reserved for one single codec selected per each offered media.
12	→		PRACK	UE acknowledges the receipt of 180 response by sending PRACK
13	←		200 OK	The SS responds PRACK with 200 OK
14	←		200 OK	SS responds the INVITE with 200 OK
15	→		ACK	UE sends the ACK
16	→		NOTIFY	UE sends a NOTIFY to confirm that the call transfer has been completed
17	←		200 OK	SS responds the NOTIFY with 200 OK
18	←		BYE	SS sends a BYE to terminate its session with UE
19	→		200 OK	UE responds the BYE with 200 OK

Specific Message Contents

REFER (Step 5)

Use the default message 'MT REFER' in annex A.2.12

202 Accepted for REFER (Step 6)

Use the default message '202 Accepted' in annex A.3.3.

NOTIFY (Step 7)

Use the default message 'MO NOTIFY for refer package' in annex A.2.13 with the following exceptions:

Header/param	Value/remark
Message-body	*SIP/2.0 100 Trying*

200 OK for NOTIFY (Step 8)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

INVITE (Step 9)

Use the default message 'INVITE for MO call setup' in annex A.2.1 with the following exceptions:

Header/param	Value/remark
Request-Line	
Request-URI	SIP or Tel URI of the transfer target
To	
addr-spec	SIP or Tel URI of the transfer target
Supported	
option-tag	*100rel, precondition*

For the contents of the SDP body see test requirement details.

100 Trying for INVITE (Step 10)

Use the default message '100 Trying for INVITE' in annex A.2.2.

180 Ringing for INVITE (Step 11)

Use the default message '180 Ringing for INVITE' in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Require	
option-tag	*precondition*
Contact	
addr-spec	Different URI must be used than the one SS uses when setting up the MO call as this is supposed now to represent another UE to which the call is being forwarded. .
Message-body	SDP body copied from the received INVITE but modified as follows: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; and - For each media, the SS shall indicate only one codec which the UE also supports - optional "a=sendonly" line inverted to "a=recvonly" and vice versa - the "a=" lines describing the current and desired state of the preconditions, updated as follows: a=curr:qos local [direction-tag] (1 a=curr:qos remote [direction-tag] (2 a=des:qos mandatory local [direction-tag] (1 a=des:qos mandatory remote [direction-tag] (1 1) The value of direction-tags in this message must be the inverse from those of INVITE (both a= lines for local and remote). If the INVITE contained the direction-tag as "recv" this message must have it as "send" and vice versa. The value "sendrecv" will be kept as is. 2) The value for direction tag of curr:qos remote must be the inverse of direction tag of curr:qos local within the INVITE.

PRACK (Step 12)

Use the default message 'PRACK' in annex A.2.4.

200 OK for PRACK (Step 13)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

200 OK for INVITE (Step 14)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	Same value as in the 180 response of step 11

ACK (Step 15)

Use the default message 'ACK' in annex A.2.7.

NOTIFY (Step 16)

Use the default message 'MO NOTIFY for refer package' in annex A.2.13 with the following exceptions:

Header/param	Value/remark
Subscription-State	
substate-value	*terminated*
expires	omitted from the request
reason	*noresource*
Message-body	*SIP/2.0 200 OK*

200 OK for NOTIFY (Step 17)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

BYE (Step 18)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE (Step 19)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

15.24.5 Test requirements

SS must check that the UE sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

Step 9: the UE shall send an INVITE message with correct content. The UE shall include the following lines in the SDP body:

- All mandatory SDP lines, as specified in SDP grammar in RFC 2327 [27] appendix A, including:
  - "o=" line indicating e.g. the session identifier and the IP address of the UE;
  - "c=" line indicating the IP address of the UE for receiving the media flow;
- Media description lines for the speech media proposed by UE for the transferred call. For the speech media at least the following lines must exist within the SDP:
  - "m=" line describing the media type as audio, transport port and protocol used for media and media format as RTP/AVP;

- "b=" line proposing the application specific maximum bandwidth ("AS" modifier) for the media;
- extra "a=" line for rtpmap attribute per each dynamic payload type given in the "m=" line. The UE shall offer at least the mandatory AMR codec;
- "a=" line for fmtp attribute per each rtpmap attribute. The fmtp attribute must cover at least the following parameters defined in RFC 4867 [67] for the AMR codec:
  mode-change-capability with value 2
  max-red with a value between 0 and 65535
- an a=sendrecv line
- four "a=" lines describing the current and desired state of the preconditions, as described in RFC 3312 [31]. At this stage of the call setup the lines shall be as follows:
  a=curr:qos local sendrecv
  a=curr:qos remote none
  a=des:qos mandatory local sendrecv
  a=des:qos [none, optional or mandatory] remote [send, recv or sendrecv]
  These four "a=" lines may appear in any order.

15.25 MO Explicit Communication Transfer – Consultative Call Transfer

15.25.1 Definition and applicability

Test to verify that the transferor UE correctly performs IMS Multimedia Telephony Consultative Explicit Communication Transfer (ECT). This process is described in 3GPP TS 24.629 [104]. The test case is applicable for IMS security or early IMS security.

15.25.2 Conformance requirement

[TS 24.629 clause 4.5.2.1]:

A UE that initiates a transfer operation shall:

- Issue a REFER request in the original communications dialog, where:
  - The request URI shall contain the SIP URI of the transferee as received in the Contact header field.
  - The Refer-To header field shall indicate the public address of the transfer Target.
  - If the transferor UE has a consultation communication with the transfer Target, a Replaces header field parameter shall be added to the Refer-To URI together with a Require=replaces header field parameter.
  - The Referred-By header field can be used to indicate the identity of the transferor. When privacy was required in the original communications dialog and a Referred-By header field is included, the UE shall include a Privacy header field set to "user".

After the REFER request is accepted by the other end with a 202 (Accepted) response, the transferor UE should get notifications of how the transferee's communication setup towards the transfer Target is progressing.

When a NOTIFY request is received on the REFER dialog that indicates that the transferee and the transfer Target have successfully setup a communication, the transferor UE may terminate the original communication with the transferee UE, by sending a BYE message on the original dialog.

Reference(s)

3GPP TS 24.629 [104], clause 4.5.2.1.

15.25.3 Test purpose

1) To verify that the transferor UE puts the call on hold before the transfer with a correct exchange of SIP/SDP protocol signalling messages; and

2) To verify that the transferor UE has a consultative communication with the transfer Target UE; and

3) To verify that the transferor UE issues a correctly composed REFER request to initiate the call transfer; and

4) To verify that the transferor UE correctly processes the NOTIFYs from the transferee; and

5) To verify that the transferor UE correctly processes the BYE request releasing the call with the transfer Target UE.

15.25.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF, registered to IMS services and set up the MO call, by executing the generic test procedure in Annex C.2 or C.2a (early IMS security only) up to the last step and thereafter executing the generic test procedure in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 14 for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1).

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and MO call.

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for MTSI (Yes/No)

Support for speech (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

Support for Explicit Communication Transfer - consultative transfer (Yes/No)

Support for sending RTCP while call is being held (Yes/No)

Support for sending RTCP during the active two-way voice sessions (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-4) UE is in an active call with the SS (simulating transferee UE). Consultative Call Transfer is initiated at the UE. UE puts the ongoing call on hold with the steps defined in Annex C.8.

5-16) UE sets up an MO call with the transfer Target UE (also simulated by the SS) by performing the same steps as defined in the generic test procedure in Annex C.21.

17-20) UE puts the call with the transfer Target UE on hold with the steps defined in Annex C.8.

21) SS waits for UE to send a REFER request to the transferee UE within the existing dialog between the UE and the transferee UE.

22) SS responds to the REFER request with a valid 202 Accepted response.

23) SS sends UE an initial NOTIFY to indicate that the implicit refer subscription is pending.

24) SS waits for UE to respond to NOTIFY with valid 200 OK response.

25-28) Call between UE and the transferee UE is put on hold by SS by performing the same procedure Annex C.9 Steps 1-4.

29) SS releases call between UE and the transfer Target UE by sending a BYE request.

30) SS waits for UE to respond to the BYE request with valid 200 OK response.

31) SS sends UE the final NOTIFY to indicate that the call transfer was successfully completed.

32) SS waits for UE to respond to NOTIFY with valid 200 OK response.

33) UE may send a BYE request to release the call with the transferee UE.

34) If UE has sent a BYE request in Step 33, SS responds to this request with valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-4			Steps defined in Annex C.8	The same messages as in Annex C.8 Steps 1-4 are used.
5-16			Steps defined in Annex C.21	The same messages as in Annex C.21 are used.
17-20			Steps defined in Annex C.8	The same messages as in Annex C.8 Steps 1-4 are used.
21	→		REFER	The UE sends REFER to SS referring to the transfer Target
22	←		202 Accepted	The SS responds to REFER with 202 Accepted
23	←		NOTIFY	The SS sends initial NOTIFY for the implicit subscription created by the REFER request
24	→		200 OK	The UE responds to NOTIFY with 200 OK
25-28			Steps defined in Annex C.9	The same messages as in Annex C.9 Steps 1-4 are used.
29	←		BYE	The SS releases the call between UE and transfer Target UE with BYE
30	→		200 OK	The UE responds to BYE with 200 OK
31	←		NOTIFY	The SS sends a NOTIFY to confirm that the call transfer has been completed
32	→		200 OK	The UE responds to NOTIFY with 200 OK
33	→		BYE	Optional: UE may send BYE request to release call with transferee UE
34	←		200 OK	Optional: If the UE has sent BYE in step 33 then SS sends 200 OK for BYE

Specific Message Contents

Messages in Steps 1-4

Messages in Steps 1-4 are the same as those specified in Annex C.8.

Messages in Steps 5-16

Messages in Steps 5-16 are the same as those specified in Annex C.21 with the following exceptions:

INVITE (Step 5)

Header/param	Value/remark
Request-Line	
Request-URI	SIP URI of transfer Target UE
To	
addr-spec	SIP URI of transfer Target UE

Messages in Steps 17-20

Messages in Steps 17-20 are the same as those specified in Annex C.8 with the following exceptions:

INVITE or UPDATE (Step 17)

Header/param	Value/remark
Request-Line	
Request-URI	px_CalleeContactUri
From	
addr-spec	same value as in the first INVITE during the call setup with transfer Target at Step 5
tag	same value as in the first INVITE during the call setup with transfer Target at Step 5
To	
addr-spec	same value as in the first INVITE during the call setup with transfer Target at Step 5
tag	px_InviteToTag
Call-ID	
callid	same value as in the first INVITE during the call setup with transfer Target at Step 5

REFER (Step 21)

Use the default message 'MO REFER' in annex A.2.10 with the following exceptions:

Header/param	Value/remark
Refer-To	
Value	<public address of transfer Target?Replaces=(dialog id of the dialog between the UE and the transfer Target)&Require=replaces>
Referred-By	
Value	same value as addr-spec field in From header in the first INVITE during initial call setup (optional)
Privacy	
Value	user (shall be included if privacy was required during original communication dialog and Referred-By header field is included)

202 Accepted for REFER (Step 22)

Use the default message '202 Accepted' in annex A.3.3.

NOTIFY (Step 23)

Use the default message 'MT NOTIFY for refer package' in annex A.2.11 with the following exceptions:

Header/param	Value/remark
Message-body	*SIP/2.0 100 Trying*

200 OK for NOTIFY (Step 24)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

Messages in Steps 25-28

Messages in Steps 25-28 are the same as those specified in Annex C.9.

BYE (Step 29)

Use the default message 'BYE' in annex A.2.8 with the following exceptions:

Header/param	Value/remark
Request-Line	
Request-URI	same value as in PRACK message at Step 8 during call setup with transfer Target
Via	
sent-by	same value as in INVITE message at Step 5 during call setup with transfer Target
Route	
route-param	URIs of the Record-Route header of 183 response at Step 7 during call setup with Transfer target, in reverse order
From	
addr-spec	same value as received in INVITE message at Step 5 during call setup with transfer Target
tag	same value as received in INVITE message at Step 5 during call setup with transfer Target
To	
addr-spec	same value as received in INVITE message at Step 5 during call setup with transfer target
tag	same value as in the 183 message at Step 7 during call setup with transfer target
Call-ID	
callid	same value as received in INVITE message at Step 5 during call setup with Transfer target

200 OK for BYE (Step 30)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

NOTIFY (Step 31)

Use the default message 'MT NOTIFY for refer package' in annex A.2.11 with the following exceptions:

Header/param	Value/remark
Subscription-State	
substate-value	*Terminated*
expires	omitted from the request
reason	*Noresource*
Message-body	*SIP/2.0 200 OK*

200 OK for NOTIFY (Step 32)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

BYE (Step 33, Optional)

Use the default message 'BYE' in annex A.2.8 with the following exceptions:

Header/param	Value/remark
Request-Line	
Request-URI	same value as in PRACK message during initial call setup with transferee
Via	
sent-by	same value as in INVITE message during initial call setup with transferee
Route	
route-param	URIs of the Record-Route header of 183 response during initial call setup with transferee, in reverse order
From	
addr-spec	same value as received in INVITE message during initial call setup with transferee
Tag	same value as received in INVITE message during initial call setup with transferee
To	
addr-spec	same value as received in INVITE message during initial call setup with transferee
Tag	same value as in the 183 message during initial call setup with transferee
Call-ID	
callid	same value as received in INVITE message during initial call setup with transferee

200 OK for BYE (Step 34) Optional step used when UE sent BYE at Step 33

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

15.25.5 Test requirements

SS must check that if the UE uses IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

15.26 MT Explicit Communication Transfer – Consultative Call Transfer (without 3PCC)

15.26.1 Definition and applicability

Test to verify that the transferee UE correctly performs IMS Multimedia Telephony Consultative Explicit Communication Transfer. This process is described in 3GPP TS 24.29 [104]. The test case is applicable for IMS security or early IMS security.

15.26.2 Conformance requirement

[TS 24.629 clause 4.5.2.5.1]:

When a REFER request is received in the context of a call transfer scenario (see subclause 4.5.2.4.1), the transferee UE shall perform the following steps:

1) apply the procedure for holding the active communication with the transferor as described in 3GPP TS 24.610 [8] clause 4.5.2.1; and

2) apply normal REFER handling procedures according to 3GPP TS 24.229 [1].

Reference(s)

3GPP TS 24.629 [104], clause 4.5.2.5.1.

15.26.3 Test purpose

1) To verify that the transferee UE puts the active communication with the transferor UE on hold with a correct exchange of SIP/SDP protocol signalling messages; and

2) To verify that the transferee UE correctly processes the REFER request from the transferor UE and sets up a communication with the transfer Target UE with a correct exchange of SIP/SDP protocol signalling messages; and

3) To verify that the transferee UE correctly processes a BYE request from the transferor UE after successful communication setup between the transferee UE and the transfer Target UE.

15.26.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has discovered P-CSCF, registered to IMS services and set up the MO call, by executing the generic test procedure in Annex C.2 or C.2a (early IMS security only) up to the last step and thereafter executing the generic test procedure in TS 36.508 [94] table 4.5A.6.3-1 steps 1 to 14 for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1). SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and MO call.

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for MTSI (Yes/No)

Support for speech (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

Support for Explicit Communication Transfer - consultative transfer (Yes/No)

Support for sending RTCP while call is being held (Yes/No)

Support for suppressing RTCP during the active two-way voice sessions (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-4) SS puts active call with UE on hold by performing the same procedure as in Annex C.9.

5) SS sends UE a REFER message to initiate transfer to the transfer Target UE.

6) SS waits for UE to respond to REFER message with 202 Accepted.

7) SS waits for UE to send an initial NOTIFY to indicate that the implicit refer subscription is pending.

8) SS responds to NOTIFY with valid 200 OK response.

9-12) UE puts active call on hold by performing the same procedure as in with the steps defined in Annex C.8.

13) SS waits for UE to send an INVITE to set up an MO call with the transfer Target UE.

14-20) If in the INVITE sent a Step 13, UE has not already indicated to have met the local preconditions, the same procedure as in Annex C.21 Steps 3-9 is performed.

21-24) Call setup with the transfer Target UE is completed by performing the same procedure as in Annex C.21 Steps 10-13.

25) SS waits for UE to send a NOTIFY message indicating 200 OK status.

26) SS responds to NOTIFY with valid 200 OK response.

27) SS releases call between transferor UE and UE by sending a BYE request.

28) SS waits for UE to respond to BYE request with valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-4			Steps defined in Annex C.9	The same messages as in Annex C.9 are used
5	←		REFER	The SS sends REFER to initiate transfer to Transfer Target UE
6	→		202 Accepted	The UE responds to REFER with 202 Accepted
7	→		NOTIFY	The UE sends initial NOTIFY for the implicit subscription created by the REFER request
8	←		200 OK	The SS responds to NOTIFY with 200 OK
9-12			Steps defined in Annex C.8	The same messages as in Annex C.8 Steps 1-4 are used
13	→		INVITE	UE sends INVITE to setup call with transfer Target UE. The UE might already indicate to have met the local preconditions
14-20			Steps 2-8 of Annex C.21	Optional steps: The same messages as in Annex C.21 Steps 3-9 are used
21-24			Steps 9-12 of Annex C.21	The same messages as in Annex C.21 Steps 10-13 are used
25	→		NOTIFY	The UE sends a NOTIFY to confirm that the call transfer has been completed
26	←		200 OK	The SS responds to NOTIFY with 200 OK
27	←		BYE	The SS releases the call between transferor UE and UE with BYE
28	→		200 OK	The UE sends 200 OK for BYE

Specific Message Contents

Messages in Steps 1-4

Messages in Steps 1-4 are the same as those specified in Annex C.9.

REFER (Step 5)

Use the default message 'MT REFER' in annex A.2.12 with the following exceptions:

Header/param	Value/remark
Refer-To	
Value	<public address of transfer Target ?Replaces=(dialog id for the call between the SS and the transfer Target)&Require=replaces>
Referred-By	
Value	same value as addr-spec field in To header in the first INVITE during initial call setup

202 Accepted (Step 6)

Use the default message '202 Accepted for REFER' in annex A.3.3.

NOTIFY (Step 7)

Use the default message 'MO NOTIFY for refer package' in annex A.2.13 with the following exceptions:

Header/param	Value/remark
Message-body	*SIP/2.0 100 Trying*

200 OK for NOTIFY (Step 8)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

Messages in Steps 9-12

Messages in Steps 9-12 are the same as those specified in Annex C.8.

INVITE (Step 13)

Same message as that specified in Annex C.21 Step 2, with the following exceptions:

Header/param	Value/remark
Request-Line	
Request-URI	<public address of transfer Target?Replaces=(dialog id of the dialog between the SS and the transfer Target)&Require=replaces>
To	
addr-spec	<public address of transfer Target?Replaces=(dialog id of the dialog between the SS and the transfer Target)&Require=replaces>

Messages in Steps 14-20, optional steps used when the UE has not already indicated to have met the local preconditions in the INVITE sent at Step 13

Messages in Steps 14-20 are the same as those specified in Annex C.21 Steps 3-9.

Messages in Steps 21-24

Messages in Steps 21-24 are the same as those specified in Annex C.21 Steps 10-13.

NOTIFY (Step 25)

Use the default message 'MO NOTIFY for refer package' in annex A.2.13 with the following exceptions:

Header/param	Value/remark
Subscription-State	
substate-value	*terminated*
expires	omitted from the request
reason	*noresource*
Message-body	*SIP/2.0 200 OK*

200 OK for NOTIFY (Step 26)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

BYE (Step 27)

Use the default message 'BYE' in annex A.2.8 with the following exceptions:

Header/param	Value/remark
Request-Line	
Request-URI	same value as in PRACK message during initial call setup
Via	
sent-by	same value as in INVITE message during initial call setup
Route	
route-param	URIs of the Record-Route header of 183 response during initial call setup, in reverse order
From	
addr-spec	same value as received in INVITE message during initial call setup
tag	same value as received in INVITE message during initial call setup
To	
addr-spec	same value as received in INVITE message during initial call setup
tag	same value as in the 183 message during initial call setup, in reverse order
Call-ID	
callid	same value as received in INVITE message during initial call setup

200 OK for BYE (Step 28)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

15.26.5 Test requirements

SS must check that if the UE uses IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

15.27 Communication Waiting and answering the call

15.27.1 Definition and applicability

Test to verify that the MT UE correctly performs MTSI Communication Waiting. This process is described in 3GPP TS 24.615 [95]. The test case is applicable for IMS security or early IMS security.

15.27.2 Conformance requirement

Generic requirements for Communication Waiting can be found in Subclause 4.5.5.3.2, 4.5.5.3.3, 4.5.5.3.4 of TS 24.615.

[TS 24.615 subclause 4.5.5.3.2]:

Upon receipt of an INVITE request containing:

- a Content-Type header field set to "application/vnd.3gpp.cw+xml";
- a MIME body according to subclause 4.4.1 with the with the <communication-waiting-indication> element contained in the <ims-cw> root element; and
- if the maximum number of waiting communications is not reached (i.e. UDUB condition has not occurred), the UE shall:

- provide a CW indication to the user;
- send a 180 (Ringing) response to the INVITE request according to the provisional response procedures described in 3GPP TS 24.229 [2];
- optionally, if the INVITE includes an Expires header field, use the value of this header field to provide the time to expiry information of the communication waiting to the user; and
- optionally start timer T_{UE-CW};

NOTE 1: The timer T_{UE-CW} is used in order to limit the duration of the CW condition at the UE. For terminals that can provide an indication to the user that a CW condition is occurring without disturbing the active communication, this timer is not needed.

NOTE 2: RFC 5621 [9] describes conditions under which a 415 (Unsupported Media Type) response is returned.

The UE may insert an Alert-Info header field set to "<urn:alert:service:call-waiting>" according to draft-liess-dispatch-alert-info-urns [8] in the 180 (Ringing) response, according to the provisional response procedures described in 3GPP TS 24.229 [2].

[TS 24.615 subclause 4.5.5.3.3]:

Case A

If user B accepts the waiting communication and holds (per procedures in 3GPP TS 24.610 [5]) or releases (per procedures in 3GPP TS 24.229 [2]) the active communication and timer T_{UE-CW} has not expired, user B's UE shall:

- stop timer T_{UE-CW} (if it has been started);
- stop providing the CW indication to User B; and
- apply the procedures for answering the waiting communication to User B as described in 3GPP TS 24.229 [2].

Case B

If T_{UE-CW} was started and expires, user B's UE shall:

- stop providing the CW indication to User B; and
- send a 480 (Temporarily Unavailable) response towards User C, optionally including a Reason header field set to cause 19, in accordance with draft-jesske-dispatch-reason-in-responses [11].

[TS 24.615 subclause 4.5.5.3.4]:

If user B's UE receives a CANCEL request or BYE request from User C during a CW condition, user B's UE shall:

- stop timer T_{UE-CW} (if necessary);
- stop providing the CW indication to User B; and
- apply the terminating UE procedures upon receipt of CANCEL or BYE as described in 3GPP TS 24.229 [2].

If user B's UE receives a CANCEL request or BYE request from User A and during a CW condition, user B's UE shall:

- stop timer T_{UE-CW} (if necessary);
- stop providing the CW indication to User B;
- apply the terminating UE procedures upon receipt of CANCEL request or BYE request as described in 3GPP TS 24.229 [2]; and
- optionally apply the procedure for accepting the waiting communication as described in 3GPP TS 24.229 [2].

Reference(s)

3GPP TS 24.615 [95], clauses 4.5.5.3.2, 4.5.5.3.3 and 4.5.5.3.4

15.27.3 Test purpose

1) To verify that the invoking UE is able to support the terminal based communication waiting service;

2) To verify that the invoking UE sends 180 (Ringing) response with a Alert-Info header field set to "<urn:alert:service:call-waiting>" in a communication waiting process.

15.27.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF, registered to IMS services and set up the MO call, by executing the generic test procedure in Annex C.2 or C.2a (early IMS security only) up to the last step and thereafter executing the generic test procedure in Annex C.7 up to its last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and MO call.

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for MTSI (Yes/No)

Support for speech (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

Support for Communication Waiting (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

Test procedure

1-8) Execute steps 1-8 of annex C.11

9) SS shall receives 180 Ringing from the UE response with a Alert-Info header field set to "<urn:alert:service:call-waiting>".

10) SS may send PRACK to the UE to acknowledge the 180 Ringing.

11) SS may receive 200 OK for PRACK from the UE.

11a) The user terminate the previous session manually.

12) SS expects and receives 200 OK for INVITE from the UE.

13) SS sends ACK to the UE.

14) UE shall sends a BYE request after step11a. However timing of sending the BYE request is not fixedly defined and it may appear any time after step 11a.

15) SS responds to the related request with a valid 200 OK response.

NOTE: Timing of BYE is not shown in the test sequence as it might appear to the SS between any of the messages 11a and 13 or after the message 13. SS shall be prepared to respond the related request immediately after receiving it from the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-8			Steps defined in annex C.11	MTSI MT speech call
9	→		180 Ringing	The UE responds to INVITE with 180 Ringing.
10	←		PRACK	(Optional) The SS shall send PRACK only if the 180 response contains 100rel option tag within the Require header.
11	→		200 OK	(Optional) The UE acknowledges the PRACK with 200 OK.
11a				The user terminates the previous session manually
12	→		200 OK	The UE responds to INVITE with a 200 OK final response after the user answers the call.
13	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.
14	→		BYE	The UE shall send a BYE to terminate its previous session. However timing of sending the BYE request is not fixedly defined and it may appear any time after step 11a.
15	←		200 OK	The SS responds to the related request with a valid 200 OK response.

Specific Message Contents

180 Ringing (step 9)

Use the default message "180 Ringing for INVITE" in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Alert-Info	<urn:alert:service:call-waiting>

PRACK (step 10)

Use the default message "PRACK" in annex A.2.4. No content body is included in this PRACK message

200 OK (step 11)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

200 OK (step 12)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

ACK (step 13)

Use the default message "ACK" in annex A.2.7.

BYE (step 14)

Use the default message "BYE" in annex A.2.8,

200 OK (step 15)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

15.27.5 Test requirements

SS must check that if the UE uses IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

The UE shall send requests and responses as described in clause 15.27.4.

15.28 Communication Waiting and cancelling the call

15.28.1 Definition and applicability

Test to verify that the UE correctly performs IMS Multimedia Telephony Communication Waiting (CW) terminal based procedure. This process is described in 3GPP TS 24.615 [95]. The test case is applicable for IMS security or early IMS security.

15.28.2 Conformance requirement

[TS 24.615 clause 1]:

The **Communication Waiting (CW)** service enables a user to be informed, that very limited resources are available for an incoming communication. The user then has the choice of accepting, rejecting or ignoring the waiting call (as per basic call procedures).

[TS 24.615 clause 4.2.1]:

When a communication arrives at the destination user, the UE validates the status of the user. If the user is already involved in one or more communications, the terminal notifies the served user of a communication waiting situation.

[TS 24.615 clause 4.5.5.3.2]:

The UE may insert an Alert-Info header field set to "<urn:alert:service:call-waiting>" according to draft-liess-dispatch-alert-info-urns [8] in the 180 (Ringing) response, according to the provisional response procedures described in 3GPP TS 24.229.

[TS 24.615 clause 4.5.5.3.4]:

If user B's UE receives a CANCEL request or BYE request from User C during a CW condition, user B's UE shall:

- stop timer T_{UE-CW} (if necessary);
- stop providing the CW indication to User B; and
- apply the terminating UE procedures upon receipt of CANCEL or BYE as described in 3GPP TS 24.229.

Reference(s)

3GPP TS 24.615 [95] clauses 1, 4.2.1, 4.5.5.3.2 and 4.5.5.3.4

15.28.3 Test purpose

1) To verify that the UE sends a correctly composed Alert-Info header field within its 180 Ringing response, if the user is involved with another IMS session when the INVITE request reaches the UE; and
2) To verify that the UE notifies the user with CW indication while the communication waiting state persists; and
3) To verify that the UE will correctly handle the incoming CANCEL request terminating the INVITE transaction.

15.28.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF, registered to IMS services and set up the MO call, by executing the generic test procedure in Annex C.2 or C.2a (early IMS security only) up to the last step and thereafter executing the generic test procedure in Annex C.21 up to its last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and MO call.

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for MTSI (Yes/No)

Support for speech (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

Support for Communication Waiting (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

Test procedure

1-8) Execute steps 1-8 of annex C.11

9) SS shall receive 180 Ringing from the UE. UE shall give communication waiting notification to the user.

10) SS may send PRACK to the UE to acknowledge the 180 Ringing.

11) SS may receive 200 OK for PRACK from the UE.

12) After 5 seconds SS sends a CANCEL request to terminate the pending INVITE transaction

13) SS expects and receives 200 OK for CANCEL from the UE.

14) SS expects and receives 487 Request Terminated for INVITE from the UE.

15) SS sends ACK to the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-8			Steps defined in annex C.11	MTSI MT speech call
9	→		180 Ringing	The UE responds to INVITE with 180 Ringing.
10	←		PRACK	(Optional) SS shall send PRACK only if the 180 response contains 100rel option tag within the Require header.
11	→		200 OK	(Optional) The UE acknowledges the PRACK with 200 OK.
12	←		CANCEL	SS sends CANCEL request to terminate the INVITE transaction
13	→		200 OK	The UE acknowledges the CANCEL with 200 OK.
14	→		487 Request Terminated	The UE responds to INVITE with a 487 Request Terminated final response after transaction was terminated.
15	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.

NOTE: The default messages contents in annex A are used with condition 'IMS security' or 'early IMS security' when applicable.
Steps 13 and 14 can occur in any order.

Specific Message Content

180 Ringing (step 9)

Use the default message "180 Ringing for INVITE" in annex A.2.6 with the following exception:

The response shall contain Alert-Info header field with value "<urn:alert:service:call-waiting>"

PRACK (step 10)

Use the default message "PRACK" in annex A.2.4. No content body is included in this PRACK message

200 OK (step 11)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

CANCEL (step 12)

Use the default message "CANCEL" in annex A.2.15.

200 OK (step 13)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

487 Request Terminated (step 14)

Use the default message "487 Request Terminated" in annex A.2.16.

ACK (step 15)

Use the default message "ACK" in annex A.2.7.

15.28.5 Test requirements

The UE shall send requests and responses as described in clause 15.28.4.

UE shall notify the user about communication waiting until the INVITE transaction is terminated by CANCEL.

16 Codec selecting

16.1 Speech AMR, indicate all codec modes

16.1.1 Definition and applicability

Test to verify that the UE correctly performs IMS Multimedia Telephony speech call setup when all AMR codec modes are offered. This process is described in 3GPP TS 24.173 [65], TS 24.229 [10] and TS 26.114 [66]. The test case is applicable for IMS security orGIBA.

16.1.2 Conformance requirement

[TS 24.229, clause 5.1.4.1]

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires local resource reservation.

NOTE 1: The terminating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

If local resource reservation is required at the terminating UE and the terminating UE supports the precondition mechanism, and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header or Require header, the terminating UE shall make use of the precondition mechanism and shall indicate a Require header with the "precondition" option-tag in any response or subsequent request it sends towards to the originating UE; or

…

[TS 26.114, clause 5.2.1]

MTSI terminals offering speech communication shall support:

- AMR speech codec (3GPP TS 26.071, 3GPP TS 26.090, 3GPP TS 26.073 and 3GPP TS 26.104) including all 8 modes and source controlled rate operation 3GPP TS 26.093. The terminal shall be capable of operating with any subset of these 8 codec modes.

[TS 24.229, clause 6.1.1]

During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261.

[TS 26.114, clause 6.2.5]

The SDP shall include bandwidth information for each media stream and also for the session in total. The bandwidth information for each media stream and for the session is defined by the Application Specific (AS) bandwidth modifier as defined in RFC 4566.

[TS 26.114, clause 7.3.1]

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556.

Reference(s)

3GPP TS 24.229[10] clauses 5.1.4.1. TS 26.114 [66] clause 5.2.1, 6.2.5, and7.3.1.

16.1.3 Test purpose

1) To verify that, when initiating MT MTSI speech AMR call and SS has resources available, the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

4) To verify that the UE is able to release the call.

16.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

GIBA (Yes/No)

Support for initiating a session (Yes/No)

Support for speech (Yes/No)

Support for IMS Multimedia Telephony (Yes/No)

Test procedure

1) SS sends an INVITE request to the UE.

2) Void.

3) SS may receive 100 Trying from the UE.

4) SS may receive 180 Ringing from the UE.

5) SS may send PRACK to the UE to acknowledge the 180 Ringing.

6) SS may receive 200 OK for PRACK from the UE.

6A) The UE accepts the session invite.
If 180 Ringing is not received from the UE after 5s from step 1, the MMI command shall be started to trigger the UE to accept the call.

7) SS expects and receives 200 OK for INVITE from the UE, with proper SDP as answer.

8) SS send an ACK to acknowledge receipt of the 200 OK for INVITE

9) SS sends BYE to the UE.

10) SS expects and receives 200 Ok for BYE from the UE

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with the first SDP offer.
2				Void
3	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response.
4	→		180 Ringing	(Optional) The UE responds to INVITE with 180 Ringing.
5	←		PRACK	(Optional) SS shall send PRACK if the 180 response contains 100rel option-tag in the Require header.
6	→		200 OK	(Optional) The UE acknowledges the PRACK with 200 OK.
6A				Make UE accept the speech AMR offer.
7	→		200 OK	The UE responds INVITE with 200 OK .
8	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.
9	←		BYE	The SS releases the call with BYE.
10	→		200 OK	The UE sends 200 OK for BYE.

NOTE: The default messages contents in annex A are used with condition 'IMS security ' or 'GIBA' when applicable

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9, with the following exceptions:

Header/param	Value/Remark
Supported option-tag	*precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=IMS conformance test* - *c=IN (addrtype) (connection-address for SS)* - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 99* - *b=AS:30* - *b=RS:0* - *b=RR:2000* - Attributes for media:*a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

100 Trying for INVITE (Step 3)

Use the default message '100 Trying for INVITE' in annex A.2.2

180 Ringing (Step 4)

Use the default message '180 Ringing for INVITE' in annex A.2.6 without the 'Record-Route' header and with the following exceptions:

Header/param	**Value/remark**
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	Contents if header Content-Type is present: length of message-body
Message-body	Header optional Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o=-* (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=IMS conformance test* - *c=IN (addrtype) (connection-address for UE)* [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 2] - *a=fmtp:*(format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be '/1' or omitted.

PRACK (step 5)

Use the default message "PRACK" in annex A.2.4. No content body is included in this PRACK message

200 OK (Step 6)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

200 OK for INVITE (Step 7)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	Contents if header Content-Type is present: length of message-body
Message-body	Header not present if 180 Ringing (step 4) contained SDP. Header present if 180 Ringing (step 4) did not contain SDP. Contents if present: The same requirements for SDP types and values as specified in step 4.

ACK (Step 8)

Use the default message 'ACK' in annex A.2.7.

BYE (step 9)

Use the default message "BYE" in annex A.2.8.

200 OK (step 10)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

16.1.5 Test requirements

The UE shall send requests and responses as described in clause 16.1.4.

16.2 Speech AMR, indicate selective codec modes

16.2.1 Definition and applicability

Test to verify that the UE correctly performs IMS Multimedia Telephony speech call setup when selective AMR codec modes are offered. This process is described in 3GPP TS 24.173 [65], TS 24.229 [10] and TS 26.114 [66]. The test case is applicable for IMS security orGIBA

.

16.2.2 Conformance requirement

Same as 34.229-1 clause 16.1.2.

16.2.3 Test purpose

1) To verify that, when initiating MT MTSI speech AMR call with selective codec modes and SS has resources available, the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

4) To verify that the UE is able to release the call.

16.2.4 Method of test

Same as 34.229-1 clause 16.1.4 except

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9, with the following exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o= - 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 99* - *b=AS:30* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-set=0,2,5,7; mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

180 Ringing (Step 4)

Use the default message '180 Ringing for INVITE' in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	Contents if header Content-Type is present: length of message-body
Message-body	Header optional Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o=-* (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 2] - *a=fmtp:*(format) *mode-set=0,2,5,7;* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be '/1' or omitted.

200 OK for INVITE (Step 7)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	Contents if header Content-Type is present: length of message-body
Message-body	Header not present if 180 Ringing (step 4) contained SDP. Header present if 180 Ringing (step 4) did not contain SDP. Contents if present: The same requirements for SDP types and values as specified in step 4.

16.2.5 Test requirements

The UE shall send requests and responses as described in clause 16.2.4.

16.3 Speech AMR-WB, indicate all codec modes

16.3.1 Definition and applicability

Test to verify that the UE correctly performs IMS Multimedia Telephony speech call setup when all AMR-WB codec modes are offered. This process is described in 3GPP TS 24.173 [65], TS 24.229 [10] and TS 26.114 [66]. The test case is applicable for IMS security orGIBA.

16.3.2 Conformance requirement

[TS 24.229, clause 5.1.4.1]

If an initial INVITE request is received the terminating UE shall check whether the terminating UE requires local resource reservation.

NOTE 1: The terminating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

If local resource reservation is required at the terminating UE and the terminating UE supports the precondition mechanism, and:

a) the received INVITE request includes the "precondition" option-tag in the Supported header or Require header, the terminating UE shall make use of the precondition mechanism and shall indicate a Require header with the "precondition" option-tag in any response or subsequent request it sends towards to the originating UE; or

…

[TS 26.114, clause 5.2.1]

MTSI terminals offering speech communication shall support:

- AMR speech codec (3GPP TS 26.071, 3GPP TS 26.090, 3GPP TS 26.073 and 3GPP TS 26.104) including all 8 modes and source controlled rate operation 3GPP TS 26.093. The terminal shall be capable of operating with any subset of these 8 codec modes.

…

MTSI terminals offering wideband speech communication at 16 kHz sampling frequency shall support:

- AMR wideband codec (3GPP TS 26.171, 3GPP TS 26.190, 3GPP TS 26.173 and 3GPP TS 26.204) including all 9 modes and source controlled rate operation 3GPP TS 26.193. The terminal shall be capable of operating with any subset of these 9 codec modes.

…

MTSI terminals offering wideband speech communication shall also offer narrowband speech communications. When offering both wideband speech and narrowband speech communication, wideband shall be listed as the first payload type in the m line of the SDP offer (RFC 4566).

[TS 24.229, clause 6.1.1]

During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261.

[TS 26.114, clause 6.2.5]

The SDP shall include bandwidth information for each media stream and also for the session in total. The bandwidth information for each media stream and for the session is defined by the Application Specific (AS) bandwidth modifier as defined in RFC 4566.

[TS 26.114, clause 7.3.1]

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556.

Reference(s)

3GPP TS 24.229[10] clauses 5.1.4.1, TS 26.114 [66] clause 5.2.1, 6.2.5 and 7.3.1.

16.3.3 Test purpose

1) To verify that, when initiating MT MTSI speech AMR-WB call and SS has resources available, the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

4) To verify that the UE is able to release the call.

16.3.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (GIBA only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

GIBA (Yes/No)

Support for initiating a session (Yes/No)

Support for speech (Yes/No)

Support for speech, AMR wideband (Yes/No)

Support for IMS Multimedia Telephony (Yes/No)

Test procedure

1) SS sends an INVITE request to the UE.

2) Void.

3) SS may receive 100 Trying from the UE.

4) SS may receive 183 Session Progress from the UE.

5) SS may send PRACK to the UE to acknowledge the 183 Session Progress.

6) SS may receive 200 OK for PRACK from the UE.

7) SS may send UPDATE to the UE

8) SS may receive 200 OK for UPDATE from the UE, with proper SDP as answer.

9) SS may receive 180 Ringing from the UE.

10) SS may send PRACK to the UE to acknowledge the 180 Ringing.

11) SS may receive 200 OK for PRACK from the UE.

11A) The UE accepts the session invite.
If 180 Ringing is not received from the UE after 5s from step 1, the MMI command shall be started to trigger the UE to accept the call.

12) SS expects and receives 200 OK for INVITE from the UE.

13) SS send an ACK to acknowledge receipt of the 200 OK for INVITE

14) SS sends BYE to the UE.

15) SS expects and receives 200 Ok for BYE from the UE

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with the first SDP offer.
2				Void
3	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response.
4	→		183 Session Progress	(Optional) The UE sends 183 response reliably with the SDP answer to the offer in INVITE
5	←		PRACK	(Optional) SS acknowledges if a 183 Session Progress is received.
6	→		200 OK	(Optional) The UE responds if a PRACK is sent.
7	←		UPDATE	(Optional) SS sends an UPDATE with SDP offer if a 183 Session Progress is received.
8	→		200 OK	(Optional) The UE acknowledges if an UPDATE is sent.
9	→		180 Ringing	(Optional) The UE responds to INVITE with 180 Ringing.
10	←		PRACK	(Optional) SS shall send PRACK if the 180 response contains 100rel option-tag in the Require header.
11	→		200 OK	(Optional) The UE acknowledges the PRACK with 200 OK.
11A				Make UE accept the speech AMR offer.
12	→		200 OK	The UE responds INVITE with 200 OK .
13	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.
14	←		BYE	The SS releases the call with BYE.
15	→		200 OK	The UE sends 200 OK for BYE.

NOTE: The default messages contents in annex A are used with condition 'IMS security ' or 'GIBA' when applicable

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9, with the following exceptions:

Header/param	Value/Remark
Supported option-tag	*precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=IMS conformance test* - *c=IN (addrtype) (connection-address for SS)* - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97 99* - *b=AS:30* - *b=RS:0* - *b=RR:2000* - Attributes for media:*a=rtpmap:97 AMR-WB/16000/1* - *a=fmtp:97 mode-change-capability=2; max-red=220* - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

100 Trying for INVITE (Step 3)

Use the default message '100 Trying for INVITE' in annex A.2.2

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Status-Line	
Reason-Phrase	Not checked
Require	
option-tag	*precondition*
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o=-* (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) Attributes for preconditions: - *a=curr:qos local sendrecv* or *a=curr:qos local none* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be '/1' or omitted.

PRACK (step 5)

Use the default message "PRACK" in annex A.2.4. No content body is included in this PRACK message.

200 OK (Step 6)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

UPDATE (step 7)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111112 IN IP6* (unicast-address for SS) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97* - *b=AS:30* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:97 AMR-WB/16000/1* - *a=fmtp:97 mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* or *curr:qos remote sendrecv* [Note 1] - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: Use the value (none/sendrecv) received from 183 Session Progress and attribute a=curr:qos local.

200 OK (step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type	
media-type	*application/sdp*
Content-Length	
value	length of message-body
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o=-* (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be '/1' or omitted.

180 Ringing (Step 9)

Use the default message '180 Ringing for INVITE' in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	Contents if header Content-Type is present: length of message-body
Message-body	Header optional if 183 Session Progress is not used Header not present if 183 Session Progress is used (step 4) Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o=-* (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be '/1' or omitted.

PRACK (step 10)

Use the default message "PRACK" in annex A.2.4. No content body is included in this PRACK message

200 OK (Step 11)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

200 OK for INVITE (Step 12)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	Contents if header Content-Type is present: length of message-body
Message-body	Header not present if 183 Session Progress is used (step 4) or 180 Ringing (step 9) contained SDP. Header present if 183 Session Progress is not used (step 4) and 180 Ringing (step 9) did not contain SDP. Contents if present: The same requirements for SDP types and values as specified in step 9.

ACK (Step 13)

Use the default message 'ACK' in annex A.2.7.

BYE (step 14)

Use the default message "BYE" in annex A.2.8.

200 OK (step 15)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

16.3.5 Test requirements

The UE shall send requests and responses as described in clause 16.3.4.

16.4 Speech AMR-WB, indicate selective codec modes

16.4.1 Definition and applicability

Test to verify that the UE correctly performs IMS Multimedia Telephony speech call setup when selective AMR-WB codec modes are offered. This process is described in 3GPP TS 24.173 [65], TS 24.229 [10] and TS 26.114 [66]. The test case is applicable for IMS security orGIBA.

16.4.2 Conformance requirement

Same as 34.229-1 clause 16.3.2.

16.4.3 Test purpose

1) To verify that, when initiating MT MTSI speech AMR-WB call with selective codec modes and SS has resources available, the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

4) To verify that the UE is able to release the call.

16.4.4 Method of test

Same as 34.229-1 clause 16.3.4 except

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9, with the following exceptions:

Header/param	Value/Remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o= - 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=IMS conformance test* - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97 99* - *c= IN* (addrtype) (connection-address for SS) - *b=AS:30* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:97 AMR-WB/16000/1* - *a=fmtp:97 mode-set=0,2,5,7,8; mode-change-capability=2; max-red=220* - *a=rtpmap:99 AMR/8000/1* - *a=fmtp:99 mode-set=0,2,5,7; mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Status-Line	
Reason-Phrase	Not checked
Require	
option-tag	*precondition*
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o=-* (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) *mode-set=0,2,5,7,8;* Attributes for preconditions: - *a=curr:qos local sendrecv* or *a=curr:qos local none* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be '/1' or omitted.

UPDATE (step 7)

Use the default message "UPDATE" in annex A.2.5, but with the following exceptions:

Header/param	Value/remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o= - 1111111111 1111111112 IN IP6* (unicast-address for SS) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97* - *b=AS:30* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:97 AMR-WB/16000/1* - *a=fmtp:97 mode-set=0,2,5,7,8; mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* or *curr:qos remote sendrecv* (Note 1) - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: Use the value (none/sendrecv) received from 183 Session Progress and attribute a=curr:qos local.

200 OK (step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type	
media-type	*application/sdp*
Content-Length	
value	length of message-body
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o=-* (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c= IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) *mode-set=0,2,5,7,8;* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be '/1' or omitted.

180 Ringing (Step 9)

Use the default message '180 Ringing for INVITE' in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	Contents if header Content-Type is present: length of message-body
Message-body	Header optional if 183 Session Progress is not used Header not present if 183 Session Progress is used (step 4) Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o=-* (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c= IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) *mode-set=0,2,5,7,8;* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be '/1' or omitted.

200 OK for INVITE (Step 12)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	Contents if header Content-Type is present: length of message-body
Message-body	Header not present if 183 Session Progress is used (step 4) or 180 Ringing (step 9) contained SDP. Header present if 183 Session Progress is not used (step 4) and 180 Ringing (step 9) did not contain SDP. Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o=-* (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c= IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR-WB/16000* [Note 2] - *a=fmtp:*(format) *mode-set=0,2,5,7,8;* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be '/1' or omitted.

16.4.5 Test requirements

The UE shall send requests and responses as described in clause 16.4.4.

16.5 Void

16.6 Void

16.7 Void

16.8 Void

16.9 Void

16.10 MO MTSI Text session with MSRP

16.10.1 Definition and applicability

Test to verify that the UE correctly performs MTSI mobile originated text messaging MSRP session setup (without preconditions) and release. The test case is applicable for IMS security or GIBA.

16.10.2 Conformance requirement

[TS 24.247, clause 8.2.1]:

For the purpose of session-mode messaging and session-mode messaging conferences, the UE shall implement the role of

- an SDP offerer as described in subclause 8.3.1; and
- an SDP answerer as described in subclause 8.3.2.

...

[TS 24.247, clause 8.3.1]:

When an SDP offerer wants to create a session mode massaging session, the SDP offerer shall populate the SDP as specified in subclause 6.1 in 3GPP TS 24.229. SDP offerer shall also include:

a) a media attribute in accordance with RFC 4975; and

b) the supported MIME types in the accept-types or accept-wrapped-types attributes in accordance with RFC 4975; and

c) the address of the SDP offerer in the path attribute, in accordance with RFC 4975.

d) an a=setup attribute in accordance with draft-ietf-simple-msrp-acm.

The SDP may also include a max-size attribute. The attribute shall be formatted in accordance with RFC 4975

The SDP offerer may want to indicate to the other user(s), that the SDP offerer is prepared to receive isComposing information, then it shall add the MIME type 'application/ im-iscomposing+xml to the accept type or access-wrapped types attributes.

At the receipt of the SDP answer, if the SDP answer contains an a=setup attribute with a "passive" value, the SDP offerer shall set up a TCP connection (if not already available) when an IP-CAN bearer with sufficient QoS is available.

In accordance with draft-ietf-simple-msrp-acm [18], the SDP offerer shall not include an a=connection attribute in the initial SDP offer. For file transfer, the SDP shall also include media level attributes in accordance with RFC 5547, with the exception that it shall include the file selector attribute (a=file-selector) with at least a size parameter.

When the 200 (OK) response for the last MSRP SENT is received, the SDP offerer shall close the MSRP media stream(s) for that particular file transfer, by sending an SDP offer where the m line port value for the file transfer media stream is set to zero, unless the MSRP media stream is the only stream in the SIP session, in which case a SIP BYE request shall be sent in order to terminate the SIP session.

...

[TS 24.247, clause 8.3.2]:

When receiving an SDP offer the SDP answerer shall populate the SDP answer as specified in subclause 6.1 in 3GPP TS 24.229. In addition the answerer shall include:

a) a media attribute in accordance with the received media attribute in the SDP offer; and

b) the supported MIME types in the accept-types or accept-wrapped-types attributes in accordance with RFC 4975; and

c) the MSRP URI of the SDP answerer in the path attribute in accordance with RFC 4975.

d) an a=setup attribute in accordance with draft-ietf-simple-msrp-acm [18].

The SDPmay also include a max-size attribute. The attribute shall be formatted in accordance with RFC 4975.

If SDP answerer receives the MIME type 'application/im-iscomposing+xml' in the accept-types or accept-wrapped-types attribute and the SDP answerer accepts the exchange of isComposing information the SDP answerer shall add the MIME type 'application/im-iscomposing+xml' to the accept-types or access-wrapped types attributes.

If the SDP answer contains an a=setup attribute with an "active" value, the SDP answerer shall set up a TCP connection (if not already available) when an IP-CAN bearer with sufficient QoS is available.

For file transfer, the answerer shall behave in accordance with draft-ietf-mmusic-file-transfer-mech-00.

...

[TS 24.247, clause 9.2.1]:

The UE shall:

- implement the role of an MSRP sender as described in subclause 9.3.1; and
- implement the role of an MSRP receiver as described in subclause 9.3.2.

...

[TS 24.247, clause 9.3.1]:

When a MSRP sender wishes to send a message, the MSRP sender shall ensure that the message length is not longer than the max-size attribute, as received in a SDP offer or a SDP answer. Depending on the message length the message may be included in one SEND request or chunked into a number of SEND requests. The MSRP sender shall follow the procedures and rules as specified in RFC 4975, when the MSRP sender fragments a message into a number SEND requests.

The SEND request shall include the Byte-Range header. The MSRP sender shall populate the Byte-Range header fields as follows:

- the range end set to * (interruptible), to make the chunks interruptible, if the SEND request is longer than 2048 octets; and
- the total field set to the total size of the message.

The MSRP sender shall create a SEND request in accordance with RFC 4975 [9], where the value of To-Path is the MSRP URI shall be set to value of path attribute received in a SDP offer or a SDP answer.

If it is possible to exchange isComposing information, the MSRP sender may include in a SEND request an isComposing status message as defined in RFC 3994.

...

[TS 24.247, clause 9.3.2]:

When a MSRP receiver receives a SEND request, the MSRP receiver shall parse the SEND request. The MSRP receiver shall either send a response including:

a) a 200 (OK) status-code , as specified in RFC 4975, for the concerned SEND message if the parsing was successful; or

b) an appropriate status-code, as specified in RFC 4975, for the concerned SEND message if the parsing was unsuccessful.

The MSRP receiver shall send a REPORT request if this is explicit or implicit requested in the SEND request(s) belonging to the message. It shall either be:

a) a successful REPORT request including status-code 200 (OK) if a complete message is received and the Report-Success header in the SEND request was set to "yes"; or

b) an unsuccessful REPORT request including status-code other than 200 (OK) as defined in RFC 4975 if the MSRP receiver can conclude that a complete message is not received and the Report-Failure header is set to "yes" or not included. The criteria to conclude that a complete message is not received are specified in RFC 4975.

Reference(s)

3GPP TS 24.247 [87] clauses 8.2.1, 8.3.1, 8.3.2, 9.2.1, 9.3.1, 9.3.2

16.10.3 Test purpose

1) To verify that when initiating MO MTSI text messaging session for MSRP the UE performs correct exchange of SIP protocol signalling messages for setting up the session.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents for MSRP.

4) To verify that the UE is able to release the messaging session.

16.10.4 Method of test

Initial conditions

UE contains either SIM application (early IMS security), ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 or C.2a (early IMS security only) up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for text, MSRP (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Test procedure

1) MO MTSI text messaging session is initiated on the UE. SS waits the UE to send an INVITE request with a SDP offer.

2) SS responds to the INVITE request with a 100 Trying response.

3) SS responds to the INVITE request with valid 200 OK response.

4) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

5) Messaging session is released on the UE. SS waits the UE to send a BYE request.

6) SS responds to the BYE request with valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		INVITE	UE sends INVITE with a SDP offer
2	←		100 Trying	The SS responds with a 100 Trying provisional response
3	←		200 OK	The SS responds INVITE with 200 OK
4	→		ACK	The UE acknowledges the receipt of 200 OK for INVITE
5	→		BYE	The UE releases the call with BYE
6	←		200 OK	The SS sends 200 OK for BYE

NOTE: The default messages contents in annex A are used with condition 'IMS security ' or 'GIBA' when applicable

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MO Call" in annex A.2.1, with the following exceptions:

Header/param	Value/remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values shall be present. Session description: - *v*= (protocol version) - *o*=- (sess-id) (sess-version) *IN IP4 or IP6* (unicast-address for UE) - *s*= (session name) - c=(network type) (address type) (connection address of UE) [Note 1] - *b*= (bandwidth) Time description: - *t*= (time the session is active) Media description: - *m=message* (transport port) *TCP/MSRP* * - c=(network type) (address type) (connection address of UE) [Note 1] Attributes for media: - *a=accept-types:* (MIME types supported by the UE for MSRP) - *a=path*:(MSRP URI of the UE as defined within RFC 4975) - *a=setup:active* In addition to those the UE may optionally include attributes like max-size or accept-wrapped-types as defined in RFC 4975. Note 1: At least one "c=" field shall be present.

100 Trying for INVITE (Step 2)

Use the default message '100 Trying for INVITE' in annex A.2.2.

200 OK for INVITE (Step 3)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	 *application/sdp*
Content-Length value	 length of message-body
Message-body	SDP body of the 200 response copied from the received INVITE but modified as follows: Session description - IP address within the "o=" and "c=" lines updated to be the address of the SS Media description: - a=path attribute to contain the MSRP URI of the SS towards which the UE should start sending the MSRP messages - *a=setup:passive* - Transport port on the "m=" line changed to the same port as given within the MSRP URI of the SS

ACK (Step 4)

Use the default message 'ACK' in annex A.2.7.

BYE (Step 5)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE (Step 6)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

16.10.5 Test requirements

After receiving ACK from SS the UE proceeds with creating a TCP connection to the TCP port which SS allocated for the MSRP session and indicated within its SDP answer. The UE shall tear down the TCP connection down after receiving the 200 OK for BYE request.

16.11 Void

16.12 Void

16.13 Void

17 Media use cases

17.1 MO Speech, add video remove video

17.1.1 Definition and applicability

Test to verify that the UE is able to add a bidirectional video component to an ongoing IMS Multimedia telephony voice call. This process is described in 3GPP TS 24.229 [10], TS 24.173 [65] and TS 26.114 [66]. The test case is applicable for IMS security or GIBA.

17.1.2 Conformance requirement

[TS 24.173, clause 5.2]:

IMS multimedia telephony communication service can support different types of media, including media types listed in 3GPP TS 22.173. The session control procedures for the different media types shall be in accordance with 3GPP TS 24.229 and 3GPP TS 24.247, with the following addition:

a) Multimedia telephony is an IMS communication service and the P-Preferred-Service and P-Asserted-Service headers shall be treated as described in 3GPP TS 24.229. The coding of the ICSI value in the P-Preferred-Service and P-Asserted-Service headers shall be according to subclause 5.1.

[TS 24.229, clause 5.1.2A.1]:

If this is a request within an existing dialog, and the request includes a Contact header field, then the UE should insert the previously used Contact header field.

...

After the dialog is established the UE may change the dialog capabilities (e.g. add a media or request a supplementary service) if defined for the IMS communication service as identified by the ICSI value using the same dialog. Otherwise, the UE shall initiate a new initial request to the other user.

[TS 24.229, clause 5.1.3]:

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 as updated by RFC 4032.

The precondition mechanism should be supported by the originating UE.

The UE may initiate a session without the precondition mechanism if the originating UE does not require local resource reservation.

NOTE 1: The originating UE can decide if local resource reservation is required based on e.g. application requirements, current access network capabilities, local configuration, etc.

In order to allow the peer entity to reserve its required resources, an originating UE supporting the precondition mechanism should make use of the precondition mechanism, even if it does not require local resource reservation.

Upon generating an initial INVITE request using the precondition mechanism, the UE shall:

- indicate the support for reliable provisional responses and specify it using the Supported header mechanism; and
- indicate the support for the preconditions mechanism and specify it using the Supported header mechanism.

Upon generating an initial INVITE request using the precondition mechanism, the UE should not indicate the requirement for the precondition mechanism by using the Require header mechanism.

NOTE 2: If an UE chooses to require the precondition mechanism, i.e. if it indicates the "precondition" option tag within the Require header, the interworking with a remote UE, that does not support the precondition mechanism, is not described in this specification.

NOTE 3: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261. The UE can accept or reject any of the forked responses, for example, if the UE is capable of supporting a limited number of simultaneous transactions or early dialogs.

Upon successful reservation of local resources the UE shall confirm the successful resource reservation (see subclause 6.1.2) within the next SIP request.

NOTE 4: In case of the precondition mechanism being used on both sides, this confirmation will be sent in either a PRACK request or an UPDATE request. In case of the precondition mechanism not being supported on one or both sides, alternatively a reINVITE request can be used for this confirmation after a 200 (OK) response has been received for the initial INVITE request, in case the terminating UE does not support the PRACK request (as described in RFC 3262) and does not support the UPDATE request (as described in RFC 3311).

[TS 24.229, clause 6.1]:

The "integration of resource management and SIP" extension is hereafter in this subclause referred to as "the precondition mechanism" and is defined in RFC 3312 as updated by RFC 4032.

In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect the SDP payloads. Hence, the UE shall not encrypt the SDP payloads.

During session establishment procedure, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261.

...

For "video" and "audio" media types that utilize the RTP/RTCP, the UE shall specify the proposed bandwidth for each media stream utilizing the "b=" media descriptor and the "AS" bandwidth modifier in the SDP.

...

If the media line in the SDP indicates the usage of RTP/RTCP, and if the UE is configured to request an RTCP bandwidth level for the session is different than the default RTCP bandwidth as specified in RFC 3556, then in addition to the "AS" bandwidth modifier in the media-level "b=" line, the UE shall include two media-level "b=" lines, one with the "RS" bandwidth modifier and the other with the "RR" bandwidth modifier as described in RFC 3556 to specify the required bandwidth allocation for RTCP. The bandwidth-value in the b=RS: and b=RR: lines may include transport overhead as described in subclause 6.1 of RFC 3890.

For other media streams the "b=" media descriptor may be included. The value or absence of the "b=" parameter will affect the assigned QoS which is defined in 3GPP TS 29.208.

NOTE 1: In a two-party session where both participants are active, the RTCP receiver reports are not sent, therefore, the RR bandwidth modifier will typically get the value of zero.

The UE shall include the MIME subtype "telephone-event" in the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 4733.

The UE shall inspect the SDP contained in any SIP request or response, looking for possible indications of grouping of media streams according to RFC 3524 and perform the appropriate actions for IP-CAN bearer establishment for media according to IP-CAN specific procedures (see subclause B.2.2.5 for IP-CAN implemented using GPRS).

If resource reservation is needed, the UE shall start reserving its local resources whenever it has sufficient information about the media streams, media authorization and used codecs available.

NOTE 2: Based on this resource reservation can, in certain cases, be initiated immediately after the sending or receiving of the initial SDP offer.

In order to fulfil the QoS requirements of one or more media streams, the UE may re-use previously reserved resources. In this case the local preconditions related to the media stream, for which resources are re-used, shall be indicated as met.

[TS 24.229, clause 6.1.2]:

An INVITE request generated by a UE shall contain a SDP offer and at least one media description. The SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session.

If the desired QoS resources for one or more media streams have not been reserved at the UE when constructing the SDP offer, the UE shall:

- indicate the related local preconditions for QoS as not met, using the segmented status type, as defined in RFC 3312 and RFC 4032, as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1); and,

- set the related media streams to inactive, by including an "a=inactive" line, according to the procedures described in RFC 4566, unless the UE knows that the precondition mechanism is supported by the remote UE.

NOTE 1: When setting the media streams to the inactive mode, the UE can include in the first SDP offer the proper values for the RS and RR modifiers and associate bandwidths to prevent the receiving of the RTCP packets, and not send any RTCP packets.

If the desired QoS resources for one or more media streams are available at the UE when the initial SDP offer is sent, the UE shall indicate the related local preconditions as met, using the segmented status type, as defined in RFC 3312 and RFC 4032, as well as the strength-tag value "mandatory" for the local segment and the strength-tag value "optional" for the remote segment, if the UE supports the precondition mechanism (see subclause 5.1.3.1).

NOTE 2: If the originating UE does not support the precondition mechanism it will not include any precondition information in SDP.

...

Upon generating the SDP offer for an INVITE request generated after receiving a 488 (Not Acceptable Here) response, as described in subclause 5.1.3.1, the UE shall include SDP payload containing a subset of the allowed media types, codecs and other parameters from the SDP payload of all 488 (Not Acceptable Here) responses related to the same session establishment attempt (i.e. a set of INVITE requests used for the same session establishment). The UE shall

order the codecs in the SDP payload according to the order of the codecs in the SDP payload of the 488 (Not Acceptable Here) response.

NOTE 3: The UE can attempt a session establishment through multiple networks with different policies and potentially can need to send multiple INVITE requests and receive multiple 488 (Not Acceptable Here) responses from different CSCF nodes. The UE therefore takes into account the SDP contents of all the 488 (Not Acceptable Here) responses received related to the same session establishment when building a new INVITE request.

Upon confirming successful local resource reservation, the UE shall create a SDP offer in which:

- the related local preconditions are set to met, using the segmented status type, as defined in RFC 3312 and RFC 4032; and
- the media streams previously set to inactive mode are set to active (sendrecv, sendonly or recvonly) mode.

Upon receiving an SDP answer, which includes more than one codec for one or more media streams, the UE shall send an SDP offer at the first possible time, selecting only one codec per media stream.

[TS 26.114 Rel-8, clause 5.2.2]:

MTSI terminals offering video communication shall support:

ITU-T Recommendation H.263 Profile 0 Level 45.

In addition they should support:

ITU-T Recommendation H.263 Profile 3 Level 45;

MPEG-4 (Part 2) Visual Simple Profile Level 3with the following constraints:

- Number of Visual Objects supported shall be limited to 1.
- The maximum frame rate shall be 30 frames per second.
- The maximum f_code shall be 2.
- The intra_dc_vlc_threshold shall be 0.
- The maximum horizontal luminance pixel resolution shall be 352 pels/line.
- The maximum vertical luminance pixel resolution shall be 288 pels/VOP.
- If AC prediction is used, the following restriction applies: QP value shall not be changed within a VOP (or within a video packet if video packets are used in a VOP). If AC prediction is not used, there are no restrictions to changing QP value.

- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC Baseline Profile Level 1.1 with constraint_set1_flag=1 and without requirements on output timing conformance (annex C of H.264). Each sequence parameter set of H.264 (AVC) shall contain the vui_parameters syntax structure including the num_reorder_frames syntax element set equal to 0.

[TS 26.114 Rel-10, clause 5.2.2]

MTSI clients in terminals offering video communication shall support:

- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Constrained Baseline Profile (CBP) Level 1.2.

In addition they should support:

- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Constrained Baseline Profile Level 3.1.

In addition they may support:

- ITU-T Recommendation H.263 [22] Profile 0 Level 45.

[TS 26.114 Rel-8, clause 6.2.1]:

The session setup for RTP transported media shall determine for each media: IP address(es), RTP profile, UDP port number(s); codec(s); RTP Payload Type number(s), RTP Payload Format(s) and any additional session parameters.

[TS 26.114 Rel-8, clause 6.2.1a.1]

MTSI clients should support SDPCapNeg to be able to negotiate RTP profiles for all media types where AVPF is supported. MTSI clients supporting SDPCapNeg shall support the complete SDPCapNeg framework.

SDPCapNeg is described in [69]. This clause only describes the SDPCapNeg attributes that are directly applicable for the RTP profile negotiation, i.e. the tcap, pcfg and acfg attributes. TS 24.229 [7] may outline further requirements needed for supporting SDPCapNeg in SDP messages.

NOTE: This clause describes only how to use the SDPCapNeg framework for RTP profile negotiation using the tcap, pcfg and acfg attributes. Implementers may therefore (incorrectly) assume that it is sufficient to implement only those specific parts of the framework that are needed for RTP profile negotiation. Doing so would however not be future proof since future versions may use other parts of the framework and there are currently no mechanisms for declaring that only a subset of the framework is supported. Hence, MTSI clients are required to support the complete framework.

[TS 26.114 Rel-8, clause 6.2.1a.2]

For voice and real-time text, SDPCapNeg shall be used when offering AVPF the first time for a new media type in the session since the support for AVPF in the answering client is not known at this stage. For video, an MTSI client shall either offer AVPF and AVP together using SDPCapNeg, or the MTSI client shall offer only AVPF, without using SDPCapNeg. If an MTSI client has offered only AVPF for video, and then receives as response either an SDP answer where the video media component has been rejected, or an SIP 488 or 606 failure response with an SDP body indicating that only AVP is supported for video media, the MTSI client should send a new SDP offer with AVP as transport for video. Subsequent SDP offers, in a re-INVITE or UPDATE, may offer AVPF without SDPCapNeg if it is known from an earlier re-INVITE or UPDATE that the answering client supports this RTP profile. If the offer includes only AVP then SDPCapNeg does not need to be used, which can occur for: text; speech if RTCP is not used; and in re-INVITEs or UPDATEs where the RTP profile has already been negotiated for the session in a preceding INVITE or UPDATE.

When offering AVP and AVPF using SDPCapNeg, the MTSI client shall offer AVP on the media (m=) line and shall offer AVPF using SDPCapNeg mechanisms. The SDPCapNeg mechanisms are used as follows:

- The support for AVPF is indicated in an attribute (a=) line using the transport capability attribute "tcap". AVPF shall be preferred over AVP.

- At least one configuration using AVPF shall be listed using the attribute for potential configurations "pcfg".

[TS 26.114, clause 6.2.3]:

If video is used in a session, the session setup shall determine the bandwidth, RTP profile, video codec, profile and level. The "imageattr" attribute as specified in should be supported.

An MTSI terminal shall offer AVPF for all media streams containing video. RTP profile negotiation shall be done as described in clause 6.2.1a.

[TS 26.114, clause 6.2.5]:

The SDP shall include bandwidth information for each media stream and also for the session in total. The bandwidth information for each media stream and for the session is defined by the Application Specific (AS) bandwidth modifier as defined in RFC 4566.

[TS 26.114, clause 6.3]:

During session renegotiation for adding or removing media components, the SDP offerer should continue to use the same media (m=) line(s) from the previously negotiated SDP for the media components that are not being added or removed.

[TS 26.114, clause 7.3.1]

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556. Therefore, an MTSIclient shall include the "b=RS:" and "b=RR:" fields in SDP, and shall be able to interpret them.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.2A.1, 5.1.3 and 6.1, TS 24.173 [65] clause 5.2 and TS 26.114 [66], clauses 5.2.2, 6.2.1, 6.2.1a.1, 6.2.1a.2, 6.2.3, 6.2.5, 6.3 and 7.3.1.

17.1.3 Test purpose

1) To verify that when adding a video component to an ongoing IMS Multimedia Telephony voice call the UE performs correct exchange of SIP protocol signalling messages; and

2) To verify that within SIP signalling the UE performs correct SDP offer/answer exchanges for negotiating media and indicating preconditions for resource reservation (as described by 3GPP TS 24.229 [10], clause 6.1); and

3) To verify that when removing the video component from the IMS Multimedia Telephony call the UE performs correct exchange of SIP and SDP protocol messages.

17.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF, registered to IMS services and set up the MO call, by executing annex C.21.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration and MO call.

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

Support for MTSI (Yes/No)

Support for integration of resource management and SIP (use of preconditions) (Yes/No)

Support for speech (Yes/No)

Support for video (Yes/No)

Support for Speech, add/remove video (Yes/No)

IMS security (Yes/No)

GIBA (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-7) UE executes the procedures described in TS 36.508 [94] table 4.5A.11.3-1, steps 1 to 7.

Test procedure

1) Add video to the voice call is initiated on the UE.

2) UE to sends a re-INVITE request to the SS.

3) SS responds to the re-INVITE request with a 100 Trying response.

4) SS responds to the re-INVITE request with a 183 Session in Progress response.

5) SS waits for the UE to send a PRACK request possibly containing the second SDP offer for update of precondition state.

6) SS responds to the PRACK request with valid 200 OK response.

7) SS waits for the UE to optionally send a UPDATE request containing the final SDP offer. UE will not send the UPDATE request if the PRACK within step 4 already contained the final offer with preconditions met.

8) SS responds to the UPDATE request (if UE sent one) with valid 200 OK response.

9) SS responds to the re-INVITE request with valid 200 OK response.

10) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

11) Video stream is removed from the multimedia call on the UE. SS waits the UE to send a re-INVITE request with a SDP offer indicating the removal of the video stream.

12) SS responds to the re-INVITE request with a 100 Trying response.

13) SS responds to the re-INVITE request with valid 200 OK response.

14) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for re-INVITE.

15) Call is released on the UE. SS waits the UE to send a BYE request.

16) SS responds to the BYE request with valid 200 OK response.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE attempt add IMS video to the voice call.	
2	→		INVITE	UE sends re-INVITE with a SDP offer containing media lines for both voice and video
3	←		100 Trying	The SS responds with a 100 Trying provisional response
4	←		183 Session in Progress	Optional step: If the UE has not yet reserved the resources for the additional video stream SS responds with an SDP answer indicating that SS has not reserved its resources for video.
5	→		PRACK	Optional step: UE acknowledges the receipt of 183 response with PRACK and optionally offers second SDP to indicate the changed precondition status.
6	←		200 OK	Optional step: The SS responds PRACK with 200 OK and answers the second SDP (if any) with mirroring its contents.
7	→		UPDATE	Optional step: UE sends an UPDATE after having reserved the resources for video if meeting the preconditions was not already indicated in step 1 or 4.
8	←		200 OK	Optional step : The SS responds UPDATE with 200 OK and indicates having reserved the resources
9	←		200 OK	The SS responds re-INVITE with 200 OK and provides its final SDP answer if steps 3-7 were omitted
10	→		ACK	The UE acknowledges the receipt of 200 OK for INVITE
11	→		INVITE	UE sends re-INVITE with a SDP offer indicating that the video component is removed from the call
12	←		100 Trying	The SS responds with a 100 Trying provisional response
13	←		200 OK	The SS responds re-INVITE with 200 OK
14	→		ACK	The UE acknowledges the receipt of 200 OK for re-INVITE
15	→		BYE	The UE releases the call with BYE
16	←		200 OK	The SS sends 200 OK for BYE

NOTE: The default messages contents in annex A are used with condition 'IMS security' or 'GIBA' when applicable

Specific Message Contents

INVITE (Step 2)

Use the default message 'INVITE for MO Call' in annex A.2.1 with condition A5 (re-INVITE within a dialog) and the following exceptions:

Header/param	Value/Remark
Supported	
option-tag	*precondition*

Message-body	The following SDP types and values. Session description: - *v=0* - *o=-* (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s=*(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t=* (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000* [Note 3] - *a=fmtp:* (format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Media description: - *m=video (transport port) RTP/AVPF* (fmt) or RTP/AVP (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=tcap:1 RTP/AVPF* [Note 2] - *a=pcfg:1 t=1* [Note 2] - *a=rtpmap: (payload type) H264/90000* - *a=fmtp: (format) profile-level-id=42e00c; sprop-parameter \ sets=J0LgDJWgUH6Af1A=,KM46gA==*

	Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The tcap/pcfg attributes are present if RTP/AVP is present on the m line. Note 3: The AMR channel number shall be '/1' or omitted.

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/Remark
Supported	
option-tag	*precondition*

Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for UE) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio (transport port) RTP/AVP* (fmt) [Note 1] - *b=AS:* (bandwidth-value) [Note 1] - *b=RS:* (bandwidth-value) [Note 1] - *b=RR:* (bandwidth-value) [Note 1] Attributes for media: - *a=rtpmap:* (payload type) AMR/8000/1 [Note 1] - *a=fmtp:* (format) mode-change-capability=2; max-red=220 [Note 1] - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Media description: - *m=video (transport port) RTP/AVPF* (fmt) [Note 1] - *b=AS:* (bandwidth-value) [Note 1] - *b=RS:* (bandwidth-value) [Note 1] - *b=RR:* (bandwidth-value) [Note 1] Attributes for media: - *a=acfg:1 t=1* [Note 2] - *a=rtpmap: (payload type)* [Note 1] - *a=fmtp: (format)* [Note 1] Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv*

	Note 1: The value for fmt, bandwidth, payload type and format copied from step 2 Note 2: Present if tcap/pcfg attributes were included in step 2.

PRACK (Step 5)

Use the default message 'PRACK' in annex A.2.4 with the exceptions:

Header/param	Value/Remark
Message-body	Header optional Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o=-* (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) [Note 2] - *s=*(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio (transport port) RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000* [Note 3] - *a=fmtp:* (format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Media description: - *m=video (transport port) RTP/AVPF* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap: (payload type) H264/90000* - *a=fmtp: (format) profile-level-id=42e00c; sprop-parameter* \ *sets=J0LgDJWgUH6Af1A=,KM46gA==*

	Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The sess-version shall been increased. Note 3: The AMR channel number shall be '/1' or omitted.

200 OK for PRACK (Step 6)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	**Value/remark**
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	Header present if Prack (step 5) contained SDP. Contents if present: SDP body of the 200 response copied from the received PRACK and modified as follows: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; Attributes for preconditions: - *a=curr:qos remote sendrecv*

UPDATE (Step 7)

Use the default message 'UPDATE' in annex A.2.5 with the following exceptions:

Header/param	**Value/remark**
Message-body	Same contents as specified in step 5.

200 OK for UPDATE (Step 8)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	**Value/remark**
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	SDP body of the 200 response copied from the received UPDATE and modified as follows: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; Attributes for preconditions: *- a=curr:qos remote sendrecv*

INVITE (Step 11)

Use the default message 'INVITE for MO Call' in annex A.2.1 with condition A5 (re-INVITE within a dialog) and the following exceptions:

Header/param	Value/Remark
Supported	
option-tag	*precondition*

Message-body	The following SDP types and values. Session description: - *v=0* - *o=-* (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s=*(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t=* (start-time) (stop-time) Media description: - *m=audio (transport port) RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:*(bandwidth-value) Attributes for media: - *a=rtpmap: (payload type)* - *a=fmtp: (format)* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Media description: - *m=video 0 RTP/AVPF* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap: (payload type)* - *a=fmtp: (format)* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos optional local sendrecv* - *a=des:qos mandatory remote sendrecv*

17.1.5 Test requirements

The UE shall send requests and responses as described in clause 17.1.4

17.2 MT Speech, add video remove video

17.2.1 Definition and applicability

Test to verify that the UE correctly add and remove media video to a mobile terminated speech session video when using IMS Multimedia Telephony. This process is described in 3GPP TS 24.229 [10], clause 5.1.2A.2, TS 24.173 [65] and TS 26.114 [66]. The test case is applicable for IMS security or GIBA.

17.2.2 Conformance requirement

[TS 24.229, clause 5.1.2A.2]

After the dialog is established the UE may change the dialog capabilities (e.g. add a media or request a supplementary service) if defined for the IMS communication service as identified by the ICSI value using the same dialog. Otherwise, the UE shall initiate a new initial request to the other user.

[TS 24.229 release 9 start, clause 6.1.1]

During the session establishment procedure, and during session modification procedures, SIP messages shall only contain SDP payload if that is intended to modify the session description, or when the SDP payload must be included in the message because of SIP rules described in RFC 3261.

[TS 24.229 release 9 end]

[TS 26.114, clause 5.2.1]

MTSI terminals offering speech communication shall support:

- AMR speech codec (3GPP TS 26.071, 3GPP TS 26.090, 3GPP TS 26.073 and 3GPP TS 26.104) including all 8 modes and source controlled rate operation 3GPP TS 26.093. The terminal shall be capable of operating with any subset of these 8 codec modes.

[TS 26.11 Rel-84, clause 5.2.2]

MTSI terminals offering video communication shall support:

ITU-T Recommendation H.263 Profile 0 Level 45.

In addition they should support:

ITU-T Recommendation H.263 Profile 3 Level 45;

MPEG-4 (Part 2) Visual Simple Profile Level 3with the following constraints:

- Number of Visual Objects supported shall be limited to 1.
- The maximum frame rate shall be 30 frames per second.
- The maximum f_code shall be 2.
- The intra_dc_vlc_threshold shall be 0.
- The maximum horizontal luminance pixel resolution shall be 352 pels/line.
- The maximum vertical luminance pixel resolution shall be 288 pels/VOP.

- If AC prediction is used, the following restriction applies: QP value shall not be changed within a VOP (or within a video packet if video packets are used in a VOP). If AC prediction is not used, there are no restrictions to changing QP value.

- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC Baseline Profile Level 1.1 with constraint_set1_flag=1 and without requirements on output timing conformance (annex C of H.264). Each sequence parameter set of H.264 (AVC) shall contain the vui_parameters syntax structure including the num_reorder_frames syntax element set equal to 0.

[TS 26.114 Rel-10, clause 5.2.2]

MTSI clients in terminals offering video communication shall support:

- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Constrained Baseline Profile (CBP) Level 1.2.

In addition they should support:

- ITU-T Recommendation H.264 / MPEG-4 (Part 10) AVC [24] Constrained Baseline Profile Level 3.1.

In addition they may support:

- ITU-T Recommendation H.263 [22] Profile 0 Level 45.

[TS 26.114, clause 6.2.1a.1]

MTSI clients should support SDPCapNeg to be able to negotiate RTP profiles for all media types where AVPF is supported. MTSI clients supporting SDPCapNeg shall support the complete SDPCapNeg framework.

SDPCapNeg is described in [69]. This clause only describes the SDPCapNeg attributes that are directly applicable for the RTP profile negotiation, i.e. the tcap, pcfg and acfg attributes. TS 24.229 [7] may outline further requirements needed for supporting SDPCapNeg in SDP messages.

NOTE: This clause describes only how to use the SDPCapNeg framework for RTP profile negotiation using the tcap, pcfg and acfg attributes. Implementers may therefore (incorrectly) assume that it is sufficient to implement only those specific parts of the framework that are needed for RTP profile negotiation. Doing so would however not be future proof since future versions may use other parts of the framework and there are currently no mechanisms for declaring that only a subset of the framework is supported. Hence, MTSI clients are required to support the complete framework.

[TS 26.114, clause 6.2.1a.2]

For voice and real-time text, SDPCapNeg shall be used when offering AVPF the first time for a new media type in the session since the support for AVPF in the answering client is not known at this stage. For video, an MTSI client shall either offer AVPF and AVP together using SDPCapNeg, or the MTSI client shall offer only AVPF, without using SDPCapNeg. If an MTSI client has offered only AVPF for video, and then receives as response either an SDP answer where the video media component has been rejected, or an SIP 488 or 606 failure response with an SDP body indicating that only AVP is supported for video media, the MTSI client should send a new SDP offer with AVP as transport for video. Subsequent SDP offers, in a re-INVITE or UPDATE, may offer AVPF without SDPCapNeg if it is known from an earlier re-INVITE or UPDATE that the answering client supports this RTP profile. If the offer includes only AVP then SDPCapNeg does not need to be used, which can occur for: text; speech if RTCP is not used; and in re-INVITEs or UPDATEs where the RTP profile has already been negotiated for the session in a preceding INVITE or UPDATE.

When offering AVP and AVPF using SDPCapNeg, the MTSI client shall offer AVP on the media (m=) line and shall offer AVPF using SDPCapNeg mechanisms. The SDPCapNeg mechanisms are used as follows:

- The support for AVPF is indicated in an attribute (a=) line using the transport capability attribute "tcap". AVPF shall be preferred over AVP.

- At least one configuration using AVPF shall be listed using the attribute for potential configurations "pcfg".

[TS 26.114, clause 6.2.3]

If video is used in a session, the session setup shall determine the bandwidth, RTP profile, video codec, profile and level. The "imageattr" attribute as specified in [76] should be supported.

An MTSI client shall offer AVPF for all media streams containing video. RTP profile negotiation shall be done as described in clause 6.2.1a.

[TS 26.114, clause 6.2.5]

The SDP shall include bandwidth information for each media stream and also for the session in total. The bandwidth information for each media stream and for the session is defined by the Application Specific (AS) bandwidth modifier as defined in RFC 4566.

[TS 26.114, clause 6.3]

During session renegotiation for adding or removing media components, the SDP offerer should continue to use the same media (m=) line(s) from the previously negotiated SDP for the media components that are not being added or removed.

[TS 26.114, clause 7.3.1]

…

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556.

…

Reference(s)

3GPP TS 24.229[10] clause 5.1.2A.2, 6.1.1 (release 9), TS 26.114 [66] clauses 5.2.1, 5.2.2, 6.2.1a.1, 6.2.1a.2, 6.2.3, 6.2.5, 6.3 and 7.3.1.

NOTE 1: Reference to a specific release is used when a corrected requirement is not updated in earlier releases of the core specifications but applies to these earlier releases.

17.2.3 Test purpose

1) To verify that media video can be added and removed when MT MTSI speech call is established.

2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.

3) To verify that within SIP signalling the UE performs the correct exchange of SDP contents.

4) To verify that the UE is able to release the call.

17.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF, registered to IMS services and established a MT MTSI speech call, by executing the generic test procedure in Annex C.11 steps 1 to 13.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Related ICS/IXIT Statement(s)

IMS security (Yes/No)

GIBA (Yes/No)

Support for initiating a session (Yes/No)

Support for video (Yes/No)

Support for speech (Yes/No)

Support for IMS Multimedia Telephony (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-6) UE executes the procedures described in TS 36.508 [94] table 4.5A.12.3-1, steps 1 to6.

Test procedure

1) SS sends a re-INVITE request to the UE.

2) Void

3) SS receives 183 Session Progress from the UE.

4) SS sends PRACK to the UE to acknowledge the 183 Session Progress.

5) SS receives 200 OK for PRACK from the UE.

6) SS sends UPDATE to the UE, with SDP indicating that precondition is met on the server side.

7) SS receives 200 OK for UPDATE from the UE.

7A) The UE accepts the session invite.

8) SS expects and receives 200 OK for re-INVITE from the UE.

9) SS sends ACK to the UE.

10) SS sends a re-INVITE to the UE with a SDP offer indicating that the video component is removed from the call.

11) SS expects and receives 200 OK for re-INVITE from the UE.

12) SS sends ACK to the UE.

13) SS sends BYE to the UE.

14) SS expects and receives 200 OK for BYE from the UE.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends re-INVITE with second SDP offer to add video.
2				Void.
3	→		183 Session Progress	The UE responds to re-INVITE by sending 183 response reliably with the SDP answer
4	←		PRACK	SS acknowledges the receipt of 183 response from the UE
5	→		200 OK	The UE acknowledges the PRACK with 200 OK.
6	←		UPDATE	SS sends an UPDATE with SDP offer indicating SS reserved resources.
7	→		200 OK	The UE acknowledges the UPDATE with 200 OK and includes SDP answer to acknowledge its current precondition status.
7A				Make UE accept the speech and video offer.
8	→		200 OK	The UE responds to the re-INVITE with a 200 OK final response.
9	←		ACK	The SS acknowledges the receipt of 200 OK for the re-INVITE.
10	←		INVITE	SS sends a re-INVITE with a SDP offer indicating that the video component is removed from the call
11	→		200 OK	The UE responds to the re-INVITE with a 200 OK final response.
12	←		ACK	The SS acknowledges the receipt of 200 OK for the re-INVITE.
13				Void
14	←		BYE	The SS sends BYE to release the call.
15	→		200 OK	The UE sends 200 OK for the BYE request and ends the call.

NOTE: The default messages contents in annex A are used with condition 'IMS security'or 'GIBA' when applicable

Specific Message Content

INVITE (Step 1)

Use the default message 'INVITE for MT Call' in annex A.2.9 with condition A5 (re-INVITE within a dialog) and the following exceptions:

Header/param	**Value/remark**
Supported	
option-tag	*precondition*

Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97* - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000/1* - *a=fmtp:* (format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Media description: - *m=video (transport port) RTP/AVPF 98* - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap: 98 H264/90000* - *a=fmtp: 98 packetization-mode=0;profile-level-id=42e00c; * *sprop-parameter-sets=J0LgDJWgUH6Af1A=,KM46gA==* - *a=rtcp-fb:* trr-int 5000* - *a=rtcp-fb:* nack* - *a=rtcp-fb:* nack pli* - *a=rtcp-fb:* ccm fir* - *a=rtcp-fb:* ccm tmmbr*

	Attributes for preconditions: *- a=curr:qos local none* *- a=curr:qos remote none* *- a=des:qos mandatory local sendrecv* *- a=des:qos optional remote sendrecv*

183 Session Progress (step 3)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	**Value/remark**
Status-Line	
Reason-Phrase	Not checked
Require	
option-tag	*precondition*

Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o=-* (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 2] - *a=fmtp:*(format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Media description: - *m=video (transport port) RTP/AVPF* (fmt) - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap: 98 H264/90000* - *a=fmtp: 98 packetization-mode=0;profile-level-id=42e00c; * *sprop-parameter-sets=J0LgDJWgUH6Af1A=,KM46gA==* Attributes for preconditions: - *a=curr:qos local none* or *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv*

	Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be '/1' or omitted.

PRACK (step 4)

Use the default message "PRACK" in annex A.2.4. No content body is included in this PRACK message.

200 OK (step 5)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

UPDATE (step 6)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	**Value/remark**

Message-body	The following SDP types and values. Session description: *- v=0* *- o=- 1111111111 1111111112 IN* (addrtype) (unicast-address for SS) *- s=IMS conformance test* *- c=IN* (addrtype) (connection-address for SS) *- b=AS:30* Time description: *-t=0 0* Media description: *- m=audio* (transport port) *RTP/AVP 97* *- b=AS:* (bandwidth-value) *- b=RS:* (bandwidth-value) *- b=RR:* (bandwidth-value) Attributes for media: *- a=rtpmap:97 AMR/8000/1* *- a=fmtp:97 mode-change-capability=2; max-red=220* Attributes for preconditions: *- a=curr:qos local sendrecv* *- a=curr:qos remote sendrecv* *- a=des:qos mandatory local sendrecv* *- a=des:qos mandatory remote sendrecv* Media description: *- m=video (transport port) RTP/AVPF 98* *- b=AS: 315* *- b=RS: 0* *- b=RR: 2500* Attributes for media: *- a=rtpmap: 98 H264/90000* *- a=fmtp: 98 packetization-mode=0;profile-level-id=42e00c; * *sprop-parameter-sets=J0LgDJWgUH6Af1A=,KM46gA==* *- a=rtcp-fb:* trr-int 5000* *- a=rtcp-fb:* nack* *- a=rtcp-fb:* nack pli* *- a=rtcp-fb:* ccm fir* *- a=rtcp-fb:* ccm tmmbr* Attributes for preconditions: *- a=curr:qos local sendrecv* *- a=curr:qos remote none* or *curr:qos remote sendrecv* [Note 1]

	- a=des:qos mandatory local sendrecv *- a=des:qos mandatory remote sendrecv* Note 1: Use the value (none/sendrecv) received from 183 Session Progress and attribute a=curr:qos local.

200 OK (step 7)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	**Value/remark**
Content-Type	
media-type	*application/sdp*
Content-Length	
value	length of message-body

Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o=-* (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 2] - *a=fmtp:*(format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Media description: - *m=video (transport port) RTP/AVPF* (fmt) - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap: 98 H264/90000* - *a=fmtp: 98 packetization-mode=0;profile-level-id=42e00c; * *sprop-parameter-sets=J0LgDJWgUH6Af1A=,KM46gA==* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be '/1' or omitted.

200 OK (Step 8)Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

ACK (step 9)

Use the default message "ACK" in annex A.2.7.

INVITE (step 10)

Use the default message 'INVITE for MT Call' in annex A.2.9 9 with condition A5 (re-INVITE within a dialog) and the following exceptions:

Header/param	**Value/remark**
Supported	
option-tag	*precondition*

Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97* - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:*(bandwidth-value) Attributes for media: - *a=rtpmap:97 AMR/8000/1* - *a=fmtp:97 mode-change-capability=2; max-red=220* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Media description: - *m=video 0 RTP/AVPF* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap: (payload type)* - *a=fmtp: (format)* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

200 OK (step 11)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

ACK (step 12)

Use the default message "ACK" in annex A.2.7.

BYE (step 14)

Use the default message "BYE" in annex A.2.8.

200 OK (step 15)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

17.2.5 Test requirements

The UE shall send requests and responses as described in clause 17.2.4

17.3 to 17.18 Void

18 SMS over IMS

18.1 Mobile Originating SMS

18.1.1 Definition and applicability

Test to verify that the UE is able to send a Mobile Originating SMS over IMS and to receive a status report. The test case is applicable for IMS security or early IMS security.

18.1.2 Conformance requirement

[TS 24.341, clause 5.3.1.2]:

When an SM-over-IP sender wants to submit an SM over IP, the SM-over-IP sender shall send a SIP MESSAGE request with the following information:

a) the Request-URI, which shall contain the PSI of the SC of the SM-over-IP sender;

NOTE 1: The PSI of the SC can be SIP URI or tel URI based on operator policy. The PSI of the SC can be obtained using one of the following methods in the priority order listed below:

1) provided by the user;

2) if UICC is used, then:

- if present in the ISIM, then the PSI of the SC is obtained from the $EF_{PSISMSC}$ in DF_TELECOM of the ISIM as per 3GPP TS 31.103 [18];

- if not present on the ISIM, then the PSI of the SC is obtained from the $EF_{PSISMSC}$ in DF_TELECOM of the USIM as per 3GPP TS 31.102 [19]; or

- if neither present on the ISIM nor on the USIM, then the PSI of the SC contains the TS-Service-Centre-Address stored in the EF_{SMSP} in DF_TELECOM as per 3GPP TS 31.102 [19]. If the PSI of the SC is based on the E.164 number from the TS-Service-Centre-Address stored in the EF_{SMSP} in DF_TELECOM then the URI constructed can be either a tel URI or a SIP URI (using the "user=phone" SIP URI parameter format).

3) if SIM is used instead of UICC, then the PSI of the SC contains the TS-Service Centre Address stored in the EF_{SMSP} in DF_TELECOM as per 3GPP TS 51.011 [20]. If the PSI of the SC is based on the E.164 number from the TS-Service-Centre-Address stored in the EF_{SMSP} in DF_TELECOM then the URI constructed can be either a tel URI or a SIP URI (using the "user=phone" SIP URI parameter format); or

4) if neither the UICC nor SIM is used, then how the PSI of the SC is configured and obtained is through means outside the scope of this specification.

b) the From header, which shall contain a public user identity of the SM-over-IP sender;

NOTE 2: The IP-SM-GW will have to use an address of the SM-over-IP sender that the SC can process (i.e. an E.164 number). This address will come from a tel URI in a P-Asserted-Identity header (as defined in RFC 3325 [13]) placed in the SIP MESSAGE request by the P-CSCF or S-CSCF.

NOTE 3: The SM-over-IP sender has to store the Call-ID of the SIP MESSAGE request, so it can associate the appropriate SIP MESSAGE request including a submit report with it.

c) the To header, which shall contain the SC of the SM-over-IP sender;

d) the Content-Type header, which shall contain "application/vnd.3gpp.sms"; and

e) the body of the request shall contain an RP-DATA message as defined in 3GPP TS 24.011 [8], including the SMS headers and the SMS user information encoded as specified in 3GPP TS 23.040 [3].

NOTE 4: The address of the SC is included in the RP-DATA message content. The address of the SC included in the RP-DATA message content is stored in the EF_{SMSP} in DF_TELECOM of the (U)SIM of the SM-over-IP sender.

NOTE 5: The SM-over-IP sender will use content transfer encoding of type "binary" for the encoding of the SM in the body of the SIP MESSAGE request.

NOTE 6: Both the address of the SC and the PSI of the SC can be configured in the $EF_{PSISMSC}$ in DF_TELECOM of the USIM and ISIM respectively using the USAT as per 3GPP TS 31.111 [21].

The SM-over-IP sender may request the SC to return the status of the submitted message. The support of status report capabilities is optional for the SC.

When a SIP MESSAGE request including a submit report in the "vnd.3gpp.sms" payload is received, the SM-over-IP sender shall:

- if SM-over-IP sender supports In-Reply-To header usage and the In-Reply-To header indicates that the request corresponds to a short message submitted by the SM-over-IP sender, generate a 200 (OK) SIP response according to RFC 3428 [14].

  if SM-over-IP sender supports In-Reply-To header usage and the In-Reply-To header indicates that the request does not correspond to a short message submitted by the SM-over-IP sender, a 488 (Not Acceptable here) SIP response according to RFC 3428 [14].

- if SM-over-IP sender does not support In-Reply-To header usage, generate a 200 (OK) SIP response according to RFC 3428 [14]; and extract the payload encoded according to 3GPP TS 24.011 [8] for RP-ACK or RP-ERROR.

[TS 24,341 clause 5.3.1.3]:

When a SIP MESSAGE request including a status report in the "vnd.3gpp.sms" payload is delivered, the SM-over-IP sender shall:

- generate a SIP response according to RFC 3428 [14];

- extract the payload encoded according to 3GPP TS 24.011 [8] for RP-DATA; and

- create a delivery report for the status report as described in subclause 5.3.2.4. The content of the delivery report is defined in 3GPP TS 24.011 [8].

[TS 24,341 clause 5.3.2.4]:

When an SM-over-IP receiver wants to send an SM delivery report over IP, the SM-over-IP receiver shall send a SIP MESSAGE request with the following information:

a) the Request-URI, which shall contain the IP-SM-GW;

NOTE 1: The address of the IP-SM-GW is received in the P-Asserted-Identity header in the SIP MESSAGE request including the delivered short message.

b) the From header, which shall contain a public user identity of the SM-over-IP receiver.

c) the To header, which shall contain the IP-SM-GW;

b) the Content-Type header shall contain "application/vnd.3gpp.sms"; and

c) the body of the request shall contain the RP-ACK or RP-ERROR message for the SM delivery report, as defined in 3GPP TS 24.011 [8].

NOTE 2: The SM-over-IP sender will use content transfer encoding of type "binary" for the encoding of the SM in the body of the SIP MESSAGE request.

Reference(s)

3GPP TS 24.341[90], clauses 5.3.1.2, 5.3.1.3 and 5.3.2.4.

18.1.3 Test purpose

1) To verify that when sending of a Mobile Originating SMS over IMS is initiated, the UE sends a SIP MESSAGE request constructed as described in 3GPP TS 24.341 [90], clause 5.3.1.2; and

2) To verify that the UE correctly handles reception of a SIP MESSAGE request including a submit report as described in 3GPP TS 24.341 [90], clause 5.3.1.2; and

3) To verify that when receiving a SIP MESSAGE request including a status report, the UE generates the correct SIP response, extracts the payload for RP-DATA and creates a delivery report as described in 3GPP TS 24.341 [90], clause 5.3.1.3.

18.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF, and registered to IMS services.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Related ICS/IXIT Statement(s)

Support for initiating a session (Yes/No)

IMS security (Yes/No)

Early IMS security (Yes/No)

Support for MO SMS over IMS(Yes/No)

Test procedure

1) Sending of a Mobile Originating SMS over IMS is initiated at the UE. The SS waits for the UE to send a SIP MESSAGE request including a vnd.3gpp.sms payload that contains the short message.

2) The SS responds to the SIP MESSAGE request with a 202 Accepted response.

3) The SS sends a SIP MESSAGE request to the UE including a vnd.3gpp.sms payload that contains a short message submission report indicating a positive acknowledgement of the short message sent by the UE at Step 1).

4) The SS waits for the UE to respond to the SIP MESSAGE request with a 200 OK response.

5) The SS sends a SIP MESSAGE request to the UE including a vnd.3gpp.sms payload that contains a status report.

6) The SS waits for the UE to respond to the SIP MESSAGE request with a 200 OK response.

7) The SS waits for the UE to send a SIP MESSAGE request including a vnd.3gpp.sms payload that contains a delivery report for the status report received at Step 5).

8) The SS responds to the SIP MESSAGE request with a 202 Accepted response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		SIP MESSAGE request	UE sends a SIP MESSAGE request including a vnd.3gpp.sms payload that contains a short message
2	←		202 Accepted	SS responds with 202 Accepted
3	←		SIP MESSAGE request	SS sends a SIP MESSAGE request including a vnd.3gpp.sms payload that contains the short message submission report indicating a positive acknowledgement of the short message sent by the UE at Step 1
4	→		200 OK	UE responds with 200 OK
5	←		SIP MESSAGE request	SS sends a SIP MESSAGE request including a vnd.3gpp.sms payload that contains a status report
6	→		200 OK	UE responds with 200 OK
7	→		SIP MESSAGE request	UE sends a SIP MESSAGE request including a vnd.3gpp.sms payload that contains a delivery report for the status report received at Step 5
8	←		202 Accepted	SS responds with 202 Accepted

NOTE: The default messages contents in annex A are used with condition 'IMS security' or 'early IMS security' when applicable

Specific Message Contents

SIP MESSAGE request (Step 1)

Use the default message 'Message for MO SMS' in Annex A.7.3

202 Accepted for SIP MESSAGE request (Step 2)

Use the default message '202 Accepted' in annex A.3.3.

SIP MESSAGE request (Step 3)

Use the default message 'Short message submission report for MO SMS' in Annex A.7.4

200 OK for SIP MESSAGE request (Step 4)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

SIP MESSAGE request (Step 5)

Use the default message 'Status Report for MO SMS' in Annex A.7.5

200 OK for SIP MESSAGE request (Step 6)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

SIP MESSAGE request (Step 7)

Use the default message 'Delivery Report for status report for MO SMS' in Annex A.7.6.

202 Accepted for SIP MESSAGE request (Step 8)

Use the default message '202 Accepted' in annex A.3.3.

18.1.5 Test requirements

SS must check that the if the UE uses full IMS security, it sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

1) In step 1, the UE shall send a SIP MESSAGE request with the following information:
   a) the Request-URI, which shall contain px_CalleeUri the PSI of the SC of the UE;
   b) the From header, which shall contain a public user identity of the UE;
   c) the To header, which shall contain the SC of the UE;
   d) the Content-Type header, which shall contain "application/vnd.3gpp.sms"; and
   e) the body of the request shall contain an RP-DATA message as defined in 3GPP TS 24.011, including the SMS headers and the SMS user information encoded as specified in 3GPP TS 23.040.
   f) Mandatory headers Via, Cseq, and max- shall be present
2) In step 4, the UE shall send a 200 OK response.
3) In Step 6, the UE shall send a 200 OK response.
4) In Step 7, the UE shall send a SIP MESSAGE request with the following information:
   a) the Request-URI, which shall contain px_CalleeUri the IP-SM-GW;
   b) the From header, which shall contain a public user identity of the UE;
   c) the To header, which shall contain the IP-SM-GW;
   d) the Content-Type header shall contain "application/vnd.3gpp.sms"; and
   e) the body of the request shall contain the RP-ACK or RP-ERROR message for the SM delivery report, as defined in 3GPP TS 24.011 [8].
   f) Mandatory headers Via, Cseq, and max- shall be present18.2 Mobile Terminating SMS

18.2 Mobile Terminating SMS

18.2.1 Definition and applicability

Test to verify that the UE correctly implemented the role of an SM-over-IP receiver.

18.2.2 Conformance requirement

[TS 24.341, clause 5.3.2.3]

When a SIP MESSAGE request including a short message in the "vnd.3gpp.sms" payload is delivered, the SM-over-IP receiver shall:

- generate a SIP response according to RFC 3428;
- extract the payload encoded according to 3GPP TS 24.011 for RP-DATA; and
- create a delivery report as described in subclause 5.3.2.4. The content of the report is defined in 3GPP TS 24.011.

[TS 24.341, clause 5.3.2.4]

When an SM-over-IP receiver wants to send an SM delivery report over IP, the SM-over-IP receiver shall send a SIP MESSAGE request with the following information:

a) the Request-URI, which shall contain the IP-SM-GW;

NOTE 1: The address of the IP-SM-GW is received in the P-Asserted-Identity header in the SIP MESSAGE request including the delivered short message.

b) the From header, which shall contain a public user identity of the SM-over-IP receiver.

c) the To header, which shall contain the IP-SM-GW;

b) the Content-Type header shall contain "application/vnd.3gpp.sms"; and

c) the body of the request shall contain the RP-ACK or RP-ERROR message for the SM delivery report, as defined in 3GPP TS 24.011 [8].

NOTE 2: The SM-over-IP sender will use content transfer encoding of type "binary" for the encoding of the SM in the body of the SIP MESSAGE request.

Reference(s)

3GPP TS 24.341[90], clause 5.3.2.3 and 5.3.2.4.

18.2.3 Test purpose

1) To verify that the UE performs correct exchange of SIP protocol signalling messages when an SM is received.
2) To verify that within SIP signalling the UE performs the correct exchange of SIP header and parameter contents.
3) To verify that within SIP signalling the UE performs the correct exchange of message body.

18.2.4 Method of test

Initial conditions

UE contains either SIM application (early IMS security), ISIM and USIM applications or only USIM application on UICC. UE has activated a PDP context, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration (IMS security).

Related ICS/IXIT Statement(s)

- UE supports SM-over-IP receiver (Yes/No)

Test procedure

1) SS sends a Short Message included in the message-body of MESSAGE.

2) UE responds with a 200 OK.

3) When the payload is extracted, the UE responds with a delivery report included in the message-body of MESSAGE.

4) SS responds with a 202 ACCEPTED.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		MESSAGE	The SS sends a Short Message.
2	→		200 OK	The UE responds with 200 OK.
3	→		MESSAGE	The UE responds with a delivery report.
4	←		202 ACCEPTED	The SS sends an accepted response.

Specific Message Contents

MESSAGE (Step 1)

Use the default message 'MESSAGE for MT SMS' in annex A.7.1.

200 OK (Step 2)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with condition A5 'Any response sent by the UE within a dialog'.

MESSAGE (Step 3)

Use the default message 'MESSAGE for delivery report' in annex A.7.2.

202 ACCEPTED (Step 4)

Use the default message '202 ACCEPTED' in annex A.3.3

18.2.5 Test requirements

The UE shall send requests and responses as described in clause 18.2.4.

19 Emergency Service over IMS

19.1 Emergency session set-up within an emergency registration

19.1.1 Emergency call with emergency registration / Success / Location information available

19.1.1.1 Definition and applicability

Test to verify that the UE can correctly register to IMS emergency services and initiate an IMS emergency call when UE is registered to IMS non-emergency services of the HPLMN either with ISIM or USIM. The process consists of setting up EPS emergency bearers, sending initial emergency registration to S-CSCF via the P-CSCF discovered, authenticating the user and finally initiating the emergency call. The test case is applicable for IMS security.

19.1.1.2 Conformance requirement

[TS 24.229 clause 4.7]:

A number of mechanisms also exist for providing location in support of emergency calls, both for routeing to a PSAP, and for use by the PSAP itself, in the IM CN subsystem:

a) by the inclusion by the UE of the Geolocation header field containing a location by reference or by value (see RFC 6442 [98]);

b) by the inclusion by the UE of a P-Access-Network-Info header field, which contains a cell identifier or location identifier, which is subsequently mapped, potentially by the recipient, into a real location;

c) by the inclusion by the P-CSCF of a P-Access-Network-Info header field based on information supplied by either the PCRF or the NASS, and which contains a cell identifier or location identifier, which is subsequently mapped, potentially by the recipient, into a real location;

d) by the allocation of a location reference that relates to the call by the LRF. Location is then supplied to the recipient over the Le interface (see 3GPP TS 23.167 [4B] for a definition of the Le interface) along with other call information. The LRF can obtain the location from entities outside the IM CN subsystem, e.g. by the e2 interface from the NASS (see ETSI TS 283 035) or from the Gateway Mobile Location Centre (GMLC).

...

Which means of providing location is used depends on local regulatory and operator requirements. One or more mechanisms can be used. Location can be subject to privacy constraints.

A number of mechanisms also exist for providing location in support of emergency calls, both for routeing to a PSAP, and for use by the PSAP itself, in the IM CN subsystem:

a) by the inclusion by the UE of the Geolocation header field containing a location by reference or by value (see RFC 6442 [89]);

b) by the inclusion by the UE of a P-Access-Network-Info header field, which contains a cell identifier or location identifier, which is subsequently mapped, potentially by the recipient, into a real location;

c) by the inclusion by the P-CSCF of a P-Access-Network-Info header field based on information supplied by either the PCRF or the NASS, and which contains a cell identifier or location identifier, which is subsequently mapped, potentially by the recipient, into a real location;

d) by the allocation of a location reference that relates to the call by the LRF. Location is then supplied to the recipient over the Le interface (see 3GPP TS 23.167 [4B] for a definition of the Le interface) along with other call information. The LRF can obtain the location from entities outside the IM CN subsystem, e.g. by the e2 interface from the NASS (see ETSI TS 283 035 [98] or from the Gateway Mobile Location Centre (GMLC).

…

Which means of providing location is used depends on local regulatory and operator requirements. One or more mechanisms can be used. Location can be subject to privacy constraints.

[TS 24.229 clause 5.1.6.1]:

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 and 3GPP TS 23.167 to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

The UE shall determine, whether it is currently attached to its home operator's network (e.g. HPLMN) or to a different network than its home operator's network (e.g. VPLMN) by applying access technology specific procedures described in the access technology specific annexes.

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 [1A] and 3GPP TS 23.167 [4B] to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

The UE shall determine, whether it is currently attached to its home operator's network (e.g. HPLMN) or to a different network than its home operator's network (e.g. VPLMN) by applying access technology specific procedures described in the access technology specific annexes.

[TS 24.229 clause 5.1.6.2]:

When the user initiates an emergency call, if emergency registration is needed (including cases described in subclause 5.1.6.2A), the UE shall perform an emergency registration prior to sending the SIP request related to the emergency call.

...

IP-CAN procedures for emergency registration are defined in 3GPP TS 23.167 and in each access technology specific annex.

When a UE performs an initial emergency registration the UE shall perform the actions as specified in subclause 5.1.1.2 with the following additions and modifications:

a) the UE shall include a "sos" SIP URI parameter in the Contact header field as described in subclause 7.2A.13, indicating that indicates that this is an emergency registration and that the associated contact address is allowed only for emergency service; and

b) the UE shall populate the From and To header fields of the REGISTER request with:

- the first entry in the list of public user identities provisioned in the UE;

- the default public user identity obtained during the normal registration, if the UE is not provisioned with a list of public user identities, but the UE is currently registered to the IM CN subsystem; and

- the derived temporary public user identity, in all other cases.

[TS 24.229 clause 5.1.6.8.3]:

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclause 5.1.2A, 5.1.3 and 5.1.4 with the following additions:

1) the UE shall insert in the INVITE request, a From header field that includes the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration, as described in subclause 4.2;

2) the UE shall include a Request-URI in the INVITE request that contains an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031. An additional sub-service type can be added if information on the type of emergency service is known;

3) the UE shall insert in the INVITE request, a To header field with:

- the same emergency service URN as in the Request-URI; or

- if the UE cannot perform local dialstring interpretation for the dialled digits, a dialstring URI representing the dialled digits in accordance with RFC 4967 or a tel URL representing the dialled digits;

NOTE 1: This version of this document does not provide any specified handling of a URI with the dialled digits in accordance with RFC 4967 at an entity within the IM CN subsystem. Behaviour when this is used is therefore not defined.

4) if available to the UE, and if defined for the access type as specified in subclause 7.2A.4, the P-Access-Network-Info header field shall contain a location identifier such as the cell id, line id or the identity of the I-WLAN access node, which is relevant for routeing the IMS emergency call;

NOTE 2: The IMS emergency specification in 3GPP TS 23.167 describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclause 5.1.2A, 5.1.3 and 5.1.4 with the following additions:

1) the UE shall insert in the INVITE request, a From header field that includes the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration, as described in subclause 4.2;

2) the UE shall include a service URN in the Request-URI of the initial INVITE request in accordance with subclause 5.1.6.8.1;

3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;

4) if available to the UE, and if defined for the access type as specified in subclause 7.2A.4, the P-Access-Network-Info header field shall contain a location identifier such as the cell id, line id or the identity of the I-WLAN access node, which is relevant for routeing the IMS emergency call;

NOTE 2: The IMS emergency specification in 3GPP TS 23.167 [4B] describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

5) the UE shall insert in the INVITE request, one or two P-Preferred-Identity header field(s) that include the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration as described in subclause 4.2;

NOTE 3: Providing two P-Preferred-Identity header fields is usually supported by UE acting as enterprise network.

6) void;

7) if the UE has its location information available, then the UE shall include its location information in the INVITE request in the following way:

- if the UE is aware of the URI that points to where the UE's location is stored, include the URI in the Geolocation header field, and set the Geolocation-Routing header field to "yes", all in accordance with RFC 6442 [98]; or

- if the geographical location information of the UE is available to the UE, include its geographical location information as PIDF location object in accordance with RFC 4119 and include the location object in a message body with the content type application/pidf+xml with RFC 6442 [98]. The Geolocation header field is set to a Content ID, set the Geolocation-Routing header field to "yes", all in accordance with RFC 6442 [98]; and

NOTE 4: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

8) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in RFC 6442 [98] in the INVITE request.

NOTE 5: RFC 3261 provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

5) the UE shall insert in the INVITE request, one or two P-Preferred-Identity header field(s) that include the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration as described in subclause 4.2;

NOTE 2: Providing two P-Preferred-Identity header fields is usually supported by UE acting as enterprise network.

6) void;

7) if the UE has its location information available, or a URI that points to the location information, then the UE shall include a Geolocation header field in the INVITE request in the following way:

- if the UE is aware of the URI that points to where the UE's location is stored, include the URI as the Geolocation header field value, as described in RFC 6442 [89]; or

- if the UE is aware of its location information, include the location information in a PIDF location object, in accordance with RFC 4119 [90], include the location object in a message body with the content type application/pidf+xml, and include a Content ID URL, referring to the message body, as the Geolocation header field value, as described RFC 6442 [89];

8) if the UE includes a Geolocation header field, the UE shall also include a Geolocation-Routing header field with a "yes" header field value, which indicates that the location of the UE can be used by other entities to make routing decisions, as described in RFC 6442 [89]; and

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

9) if the UE has neither geographical location information available, nor a URI that points to the location information, the UE shall not insert a Geolocation header field in the INVITE request.

NOTE 4: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

[TS 24.229 annex L.2.2.6]:

Emergency bearers are defined for use in emergency calls in EPS and core network support of these bearers is indicated to the UE in NAS signalling. Where the UE recognises that a call request is an emergency call and the core network supports emergency bearers, the UE shall use these EPS bearer contexts for both signalling and media for emergency calls made using the IM CN subsystem.

...

When activating a EPS bearer context to perform emergency registration, the UE shall request a PDN connection for emergency bearer services as described in 3GPP TS 24.301. The procedures for EPS bearer context activation and P-CSCF discovery, as described in subclause L.2.2.1 of this specification apply accordingly.

In order to find out whether the UE is attached to the home PLMN or to the visited PLMN, the UE shall compare the MCC and MNC values derived from its IMSI with the MCC and MNC of the PLMN the UE is attached to. If the MCC and MNC of the PLMN the UE is attached to do not match with the MCC and MNC derived from the IMSI, then for the purpose of emergency calls in the IM CN subsystem the UE shall consider to be attached to a VPLMN.

NOTE: In this respect an equivalent HPLMN, as defined in 3GPP TS 23.122 will be considered as a visited network.

[TS 24.237 clause 7.2]:

When originating an emergency call as specified in 3GPP TS 24.229 and if the SC UE has an IMEI, then the SC UE shall include the instance-id media feature tag as specified in IETF RFC 5626 with value based on the IMEI as defined in 3GPP TS 23.003 in the Contact header field of the SIP INVITE request.

[TS 23.003 clause 13.8]:

An instance-id is a SIP Contact header parameter that uniquely identifies the SIP UA performing a registration.

When an IMEI is available, the instance-id shall take the form of a IMEI URN (see draft-montemurro-gsma-imei-urn). The format of the instance-id shall take the form "urn:gsma:imei:<gsma-specifier-defined-substring>" where by the gsma-specifier-defined-substring shall be the IMEI encoded as defined in draft-montemurro-gsma-imei-urn. The optional <gsma-specifier-defined-param> parameters shall not be included in the instance-id. An example of such an instance-id is as follows:

EXAMPLE: urn:gsma:imei:90420156-025763-0

Reference(s)

3GPP TS 24.229[10], clauses 5.1.6.1, 5.1.6.2, 5.1.6.8.3 and Annex L2.2.6, TS 24.237 [110] clause 7.2 and TS 23.003 [32] clause 13.8 (release 9)

19.1.1.3 Test purpose

1) To verify that the UE is able to request activation of EPS emergency bearer contexts, according to 3GPP TS 24.229 [10] annex L.2.2.6; and

2) To verify that the UE sends a correctly composed initial SIP REGISTER request for emergency services to S-CSCF via the discovered P-CSCF, according to 3GPP TS 24.229 [10] clause 5.1.6.1; and

3) To verify that the UE is able to use the IMS security procedures for the IMS emergency registration, as defined for IMS AKA and IPSec within 3GPP TS 24.229 [10] clause 5.1.1; and

4) To verify the support of the UE for providing its location within the IMS emergency call signalling messages, as defined within 3GPP TS 24.229 [10] clause 5.1.6.8.3; and

5) To verify that the UI sends a correctly composed SIP INVITE request for the emergency call setup and will correctly complete the emergency session setup using SDP preconditions, according to 3GPP TS 24.229 [10] clauses 5.1.6.8.3 and 6.1.2.

19.1.1.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. In the E-UTRA attach SS has indicated to the UE that the cell supports E-UTRA emergency bearers. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test environment shall be set up to provide the needed input to the UE, in order for the UE to derive its location, if the UE uses Geolocation header for providing its geographical location. This shall be done by use of the test function Update UE Location Information defined in TS 34.109 [117] or in TS 36.509 [118] depending on the RAT being used in the test case, if supported by the UE according to pc_UpdateUE_LocationInformation. Otherwise, or in addition any other suitable method may also be used.

Related ICS/IXIT Statement(s)

- UE supports IMS emergency services (Yes/No)
- UE supports IPSec ESP confidentiality protection (Yes/No)
- IMS security (Yes/No)
- obtaining and using GRUUs in the Session Initiation Protocol (SIP) (Yes/No)
- UE uses Geolocation header to provide its geographical location for emergency session setup (Yes/No)
- UE supports test function Update UE Location Information (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-15) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 15 for EPS emergency bearer context activation, IMS emergency registration and subsequent IMS emergency speech call.

16) Call is released on the UE. SS waits the UE to send a BYE request.

17) SS responds to the BYE request with valid 200 OK response.

Expected sequence:

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-15			Steps defined in annex C.20 followed by the steps defined in annex C.22	IMS emergency registration by the UE followed by IMS emergency call setup with PSAP. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
16	→		BYE	The UE releases the call with BYE
17	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

INVITE (step 1 of Annex C.22)

Use the default message 'INVITE for MO call setup' in annex A.2.1. with the following conditions:

- A7 'INVITE for creating an emergency session within an emergency registration' shall apply; and
- A8 'UE uses Geolocation header to provide its geographical location for emergency session setup, has obtained its location and is setting up an emergency session ' shall apply if the UE uses Geolocation header to provide its geographical location for emergency session setup.

180 Ringing for INVITE (step 3 of Annex C.22)

Use the default message '180 Ringing for INVITE' in annex A.2.6 The condition A4 '180 sent by the SS when setting up an emergency call' shall apply.

200 OK for INVITE (step 4 of Annex C.22)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1. The condition A6 'Response sent by SS for INVITE for emergency call' shall apply

BYE (Step 16)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE (Step 17)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

19.1.1.5 Test requirements

If the UE uses Geolocation header to provide its geographical location for emergency session setup the INVITE request sent for initiating the emergency call shall contain a Geolocation header. The body of an INVITE request containing the Geolocation header must contain a PIDF location object. The PIDF-LO shall be syntactically correct (as specified within RFC 4119 [99]) and it shall be mapped to the same Content-ID which can be found from the Geolocation header.

19.1.2 Emergency call with emergency registration / Success / Location information not available

19.1.2.1 Definition and applicability

Test to verify that the UE can correctly register to IMS emergency services and initiate an IMS emergency call when UE is registered to IMS non-emergency services of the HPLMN either with ISIM or USIM. The process consists of setting up EPS emergency bearers, sending initial emergency registration to S-CSCF via the P-CSCF discovered, authenticating the user and finally initiating the emergency call. In this case the location information is not available to the UE. The test case is applicable for IMS security.

19.1.2.2 Conformance requirement

[TS 24.229 clause 5.1.6.8.3]:

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclause 5.1.2A, 5.1.3 and 5.1.4 with the following additions:

...

8) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in RFC 6442 [98] in the INVITE request.

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclause 5.1.2A, 5.1.3 and 5.1.4 with the following additions:

…

8) if the UE includes a Geolocation header field, the UE shall also include a Geolocation-Routing header field with a "yes" header field value, which indicates that the location of the UE can be used by other entities to make routing decisions, as described in RFC 6442 [89]; and

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

9) if the UE has neither geographical location information available, nor a URI that points to the location information, the UE shall not insert a Geolocation header field in the INVITE request.

Reference(s)

3GPP TS 24.229[10], clause 5.1.6.8.3 (release 9)

19.1.2.3 Test purpose

1) To verify that if the location information is not available UE will not add Geolocation header or PIDF-LO to the INVITE request for emergency call, as defined within 3GPP TS 24.229 [10] clause 5.1.6.8.3.

19.1.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. In the E-UTRA attach SS has indicated to the UE that the cell supports E-UTRA emergency bearers. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Test environment shall ensure that UE can not access any information (such as GPS signal) from which the UE would be able to derive its geographical location. The UE shall only be able to read the global cell ID as provided by the SS.

Related ICS/IXIT Statement(s)

- UE supports IMS emergency services (Yes/No)
- UE supports IPSec ESP confidentiality protection (Yes/No)
- IMS security (Yes/No)

- obtaining and using GRUUs in the Session Initiation Protocol (SIP) (Yes/No)
- UE uses Geolocation header to provide its geographical location for emergency session setup (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-15) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 15 for EPS emergency bearer context activation, IMS emergency registration and subsequent IMS emergency speech call.

16) Call is released on the UE. SS waits the UE to send a BYE request.

17) SS responds to the BYE request with valid 200 OK response.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
16	→		BYE	The UE releases the call with BYE
17	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

INVITE (Step 1 of Annex C.22)

Use the default message 'INVITE for MO call setup' in annex A.2.1. The condition A7 'INVITE for creating an emergency session within an emergency registration' shall apply. In this test case condition A8 shall not apply as the UE is not able to obtain its geographical location.

180 Ringing for INVITE (Step 3 of Annex C.22)

Use the default message '180 Ringing for INVITE' in annex A.2.6 The condition A4 '180 sent by the SS when setting up an emergency call' shall apply.

200 OK for INVITE (Step 4 of Annex C.22)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1. The condition A6 'Response sent by SS for INVITE for emergency call' shall apply

BYE (Step 16)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE (Step 17)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

19.1.2.5 Test requirements

The INVITE request sent for initiating the emergency call shall not contain a Geolocation header and the body of the request must not contain a PIDF location object.

19.1.3 Emergency call with emergency registration / Abnormal case / IM CN sends a 380 / UE performs emergency call via CS domain / UTRAN or GERAN

19.1.3.1 Definition and applicability

Test to verify that the UE performs a emergency call via CS domain, when attempt to initiate an IMS emergency call is rejected by 380 for a UE registered to IMS emergency services and IMS non-emergency services of the HPLMN either with ISIM or USIM. The process consists of setting up EPS emergency bearers, sending initial emergency registration to S-CSCF via the P-CSCF discovered, authenticating the user , initiating the emergency call. The emergency call is rejected with 380 and UE performs emergency call via supported CS domain over UTRAN or GERAN. The test case is applicable for IMS security.

19.1.3.2 Conformance requirement

[TS 24.229 clause 5.1.6.1]:

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 and 3GPP TS 23.167 to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

The UE shall determine, whether it is currently attached to its home operator's network (e.g. HPLMN) or to a different network than its home operator's network (e.g. VPLMN) by applying access technology specific procedures described in the access technology specific annexes.

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 [1A] and 3GPP TS 23.167 [4B] to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

The UE shall determine, whether it is currently attached to its home operator's network (e.g. HPLMN) or to a different network than its home operator's network (e.g. VPLMN) by applying access technology specific procedures described in the access technology specific annexes.

[TS 24.229 clause 5.1.6.2]:

When the user initiates an emergency call, if emergency registration is needed (including cases described in subclause 5.1.6.2A), the UE shall perform an emergency registration prior to sending the SIP request related to the emergency call.

...

IP-CAN procedures for emergency registration are defined in 3GPP TS 23.167 and in each access technology specific annex.

When a UE performs an initial emergency registration the UE shall perform the actions as specified in subclause 5.1.1.2 with the following additions and modifications:

a) the UE shall include a "sos" SIP URI parameter in the Contact header field as described in subclause 7.2A.13, indicating that indicates that this is an emergency registration and that the associated contact address is allowed only for emergency service; and

b) the UE shall populate the From and To header fields of the REGISTER request with:

   - the first entry in the list of public user identities provisioned in the UE;

   - the default public user identity obtained during the normal registration, if the UE is not provisioned with a list of public user identities, but the UE is currently registered to the IM CN subsystem; and

   - the derived temporary public user identity, in all other cases.

[TS 24.229 clause 5.1.6.8.1]:

The UE shall translate any user indicated emergency number as specified in 3GPP TS 22.101 [1A] to an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69]. An additional sub-service type can be added if information on the type of emergency service is known.

In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response including a 3GPP IM CN subsystem XML body as described in subclause 7.6 that includes an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.7AA), the UE shall automatically send an ACK request to the P-CSCF as per normal SIP procedures and terminate the session. In addition, if the 380 (Alternative Service) response includes a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration:

- the UE may also provide an indication to the user based on the text string contained in the <reason> child element of the <alternative-service> child element of the <ims-3gpp> element; and

- one of subclause 5.1.6.8.3 or subclause 5.1.6.8.4 applies.

NOTE 1: Emergency numbers which the UE does not detect, will be treated as a normal call.

NOTE 2: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF.

[TS 24.229 clause 5.1.6.8.3]:

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclause 5.1.2A, 5.1.3 and 5.1.4 with the following additions:

1) the UE shall insert in the INVITE request, a From header field that includes the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration, as described in subclause 4.2;

2) the UE shall include a Request-URI in the INVITE request that contains an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69]. An additional sub-service type can be added if information on the type of emergency service is known;

3) the UE shall insert in the INVITE request, a To header field with:

   - the same emergency service URN as in the Request-URI; or

   - if the UE cannot perform local dialstring interpretation for the dialled digits, a dialstring URI representing the dialled digits in accordance with RFC 4967 [103] or a tel URL representing the dialled digits;

NOTE 1: This version of this document does not provide any specified handling of a URI with the dialled digits in accordance with RFC 4967 [103] at an entity within the IM CN subsystem. Behaviour when this is used is therefore not defined.

4) if available to the UE, and if defined for the access type as specified in subclause 7.2A.4, the P-Access-Network-Info header field shall contain a location identifier such as the cell id, line id or the identity of the I-WLAN access node, which is relevant for routeing the IMS emergency call;

NOTE 2: The IMS emergency specification in 3GPP TS 23.167 [4B] describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclause 5.1.2A, 5.1.3 and 5.1.4 with the following additions:

1) the UE shall insert in the INVITE request, a From header field that includes the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration, as described in subclause 4.2;

2) the UE shall include a service URN in the Request-URI of the initial INVITE request in accordance with subclause 5.1.6.8.1;

3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;

4) if available to the UE, and if defined for the access type as specified in subclause 7.2A.4, the P-Access-Network-Info header field shall contain a location identifier such as the cell id, line id or the identity of the I-WLAN access node, which is relevant for routeing the IMS emergency call;

NOTE 2: The IMS emergency specification in 3GPP TS 23.167 [4B] describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

5) the UE shall insert in the INVITE request, one or two P-Preferred-Identity header field(s) that include the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration as described in subclause 4.2;

NOTE 3: Providing two P-Preferred-Identity header fields is usually supported by UE acting as enterprise network.

6) void;

7) if the UE has its location information available, then the UE shall include its location information in the INVITE request in the following way:

- if the UE is aware of the URI that points to where the UE's location is stored, include the URI in the Geolocation header field, and set the Geolocation-Routing header field to "yes", in accordance with RFC 6442 [98]; or

- if the geographical location information of the UE is available to the UE, include its geographical location information as PIDF location object in accordance with RFC 4119 [90] and include the location object in a message body with the content type application/pidf+xml in accordance with RFC 6442 [98]. The Geolocation header field is set to a Content ID, set the Geolocation-Routing header field to "yes", all in accordance with RFC 6442 [98]; and

NOTE 4: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

8) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in RFC 6442 [98] in the INVITE request.

NOTE 5: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

5) the UE shall insert in the INVITE request, one or two P-Preferred-Identity header field(s) that include the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration as described in subclause 4.2;

NOTE 2: Providing two P-Preferred-Identity header fields is usually supported by UE acting as enterprise network.

6) void;

7) if the UE has its location information available, or a URI that points to the location information, then the UE shall include a Geolocation header field in the INVITE request in the following way:

- if the UE is aware of the URI that points to where the UE's location is stored, include the URI as the Geolocation header field value, as described in RFC 6442 [89]; or

- if the UE is aware of its location information, include the location information in a PIDF location object, in accordance with RFC 4119 [90], include the location object in a message body with the content type application/pidf+xml, and include a Content ID URL, referring to the message body, as the Geolocation header field value, as described RFC 6442 [89];

8) if the UE includes a Geolocation header field, the UE shall also include a Geolocation-Routing header field with a "yes" header field value, which indicates that the location of the UE can be used by other entities to make routing decisions, as described in RFC 6442 [89]; and

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

9) if the UE has neither geographical location information available, nor a URI that points to the location information, the UE shall not insert a Geolocation header field in the INVITE request.

NOTE 4: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

<discussion see above>

In the event the UE receives a 380 (Alternative Service) response with a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration, and the Content-Type header field set according to subclause 7.6 (i.e. "application/3gpp-ims+xml"), independent of the value or presence of the Content-Disposition header field, independent of the value or presence of Content-Disposition parameters, then this default content disposition, identified as "3gpp-alternative-service", is applied as follows:

- if the 380 (Alternative Service) response includes a 3GPP IM CN subsystem XML body as described in subclause 7.6 the <ims-3gpp> element, including a version attribute, with the <alternative-service> child element with the <type> child element set to "emergency" (see table 7.7AA), then the UE shall perform the first action that is applicable from the following prioritised actions:

  - attempt emergency call via CS domain using appropriate access technology specific procedures, if available and not already tried;

  - if the <action> child element of the <alternative-service> child element of the <ims-3gpp> element in the IM CN subsystem XML body as described in subclause 7.6 is set to "emergency-registration" (see table 7.7AB), perform an initial emergency registration using a different VPLMN if available, as described in subclause 5.1.6.2 and if the new emergency registration succeeded, attempt an emergency call as described in this subclause; or

  - perform implementation specific actions to establish the emergency call; and

- if the 380 (Alternative Service) response includes a 3GPP IM CN subsystem XML body as described in subclause 7.6 with the <ims-3gpp> element, including a version attribute, with the <alternative-service> child element with the <type> child element set to "emergency" (see table 7.7AA) then the UE may also provide an indication to the user based on the text string contained in the <reason> child element of the <alternative-service> child element of the <ims-3gpp> element.

NOTE 6: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF.

In the event the UE receives a 380 (Alternative Service) response with a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration, and the Content-Type header field set according to subclause 7.6 (i.e. "application/3gpp-ims+xml"), independent of the value or presence of the Content-Disposition header field, independent of the value or presence of Content-Disposition parameters, then the following treatment is applied:

1) if the 380 (Alternative Service) response includes a 3GPP IM CN subsystem XML body as described in subclause 7.6 the <ims-3gpp> element, including a version attribute, with the <alternative-service> child element with the <type> child element set to "emergency" (see table 7.7AA), then the UE shall:

   a) if the CS domain is available to the UE, and no prior attempt using the CS domain for the current emergency call attempt has been made, attempt emergency call via CS domain using appropriate access technology specific procedures; and

   b) if the CS domain is not available to the UE or the emergency call has already been attempted using the CS domain, then perform one of the following actions:

      - if the <action> child element of the <alternative-service> child element of the <ims-3gpp> element in the IM CN subsystem XML body as described in subclause 7.6 is set to "emergency-registration" (see table 7.7AB), perform an initial emergency registration using a different VPLMN if available, as

described in subclause 5.1.6.2 and if the new emergency registration succeeded, attempt an emergency call as described in this subclause; or

- perform implementation specific actions to establish the emergency call; and

2) if the 380 (Alternative Service) response includes a 3GPP IM CN subsystem XML body as described in subclause 7.6 with the <ims-3gpp> element, including a version attribute, with the <alternative-service> child element with the <type> child element set to "emergency" (see table 7.7AA) then the UE may also provide an indication to the user based on the text string contained in the <reason> child element of the <alternative-service> child element of the <ims-3gpp> element.

NOTE 5: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF.

[TS 24.229 annex L.2.2.6]:

Emergency bearers are defined for use in emergency calls in EPS and core network support of these bearers is indicated to the UE in NAS signalling. Where the UE recognises that a call request is an emergency call and the core network supports emergency bearers, the UE shall use these EPS bearer contexts for both signalling and media for emergency calls made using the IM CN subsystem.

...

When activating a EPS bearer context to perform emergency registration, the UE shall request a PDN connection for emergency bearer services as described in 3GPP TS 24.301. The procedures for EPS bearer context activation and P-CSCF discovery, as described in subclause L.2.2.1 of this specification apply accordingly.

In order to find out whether the UE is attached to the home PLMN or to the visited PLMN, the UE shall compare the MCC and MNC values derived from its IMSI with the MCC and MNC of the PLMN the UE is attached to. If the MCC and MNC of the PLMN the UE is attached to do not match with the MCC and MNC derived from the IMSI, then for the purpose of emergency calls in the IM CN subsystem the UE shall consider to be attached to a VPLMN.

NOTE: In this respect an equivalent HPLMN, as defined in 3GPP TS 23.122 will be considered as a visited network.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.6.1, 5.1.6.2, 5.1.6.8.31, 5.1.6.8.3 and Annex L2.2.6 (release 9)

19.1.3.3 Test purpose

1) To verify that the on reception of 380 Alternate Service for an INVITE sent for emergency call establishment, UE initiates the emergency call in supported CS domain over UTRAN or GERAN.

19.1.3.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

The SS is configured:

-- with 2 cells: as in TS 36.508

- E-UTRAN cell 1

- if px_RATComb_Tested = EUTRA_UTRA, cell 5

- if px_RATComb_Tested = EUTRA_GERAN , GERAN cell 24
- Cell 1 power level is set as 'serving cell' and cell 24/cell 5 power level is set as 'suitable cell'

Related ICS/IXIT Statement(s)

- UE supports IMS emergency services (Yes/No)
- UE supports IPSec ESP confidentiality protection (Yes/No)
- IMS security (Yes/No)
- UE supports emergency call on CS domain (UTRAN/GERAN) (Yes/No)
- Network supports UTRAN or GERAN (px_RATComb_Tested)

Note: Setting px_RATComb_Tested = EUTRA_Only is not allowed.

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) IMS emergency call is initiated on the UE.

2)-5) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 2 to 15 and parallel behaviour steps 1-4 for EPS emergency bearer context activation, and subsequent IMS emergency registration,

6) UE sends INVITE for emergency call.

7) SS responds with 380 Alternative services. UE ACKS the 380 Alternative service message.

8) UE performs cell reselection to a cell supporting CS domain (UTRAN/GERAN) based on capability supported and after necessary MM/GMM registration, initiates CS domain emergency call.

9) CS call is established.

10) CS call is released.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			User initiates an emergency call	
2-5			Steps defined in annex C.20	EPS emergency bearer context activation and subsequent IMS emergency registration by the UE. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
6	→		INVITE	UE sends INVITE with the first SDP offer indicating all desired medias and codecs the UE supports
7	<-		380 Alternative Service	The SS responds with a 380 Alternative Service response
8	→		ACK	The UE acknowledges the receipt of 380 Alternative Service for INVITE
9			UE performs cell reselection to a cell supporting CS domain (UTRAN or GERAN cell) and performs emergency call in CS domain after MM/GMM registration (if needed)	.
10			CS call is released	

Specific Message Contents

INVITE (Step 6)

Use the default message 'INVITE for MO call setup' in annex A.2.1. with the following conditions:

- A7 'INVITE for creating an emergency session within an emergency registration' shall apply;

380 Alternative Service (Step 7)

Use the default message '380 Alternative Service' in annex A.4.1.

ACK (Step 8)

Use the default message 'ACK' in annex A.2.7.

19.1.3.5 Test requirements

In step 9, UE initiates a CS emergency call in UTRAN/GERAN cell.

19.1.3a Emergency call with emergency registration / Abnormal case / IM CN sends a 380 / UE performs emergency call via CS domain / CDMA 2000 1xRTT

19.1.3a.1 Definition and applicability

Same as in 19.1.3.1, except: UE performs emergency call via supported CS domain over CDMA 2000 1xRTT .

19.1.3a.2 Conformance requirement

Same Conformance requirement as in clause 19.1.3.2

19.1.3a.3 Test purpose

1) To verify that the on reception of 380 Alternate Service for an INVITE sent for emergency call establishment, UE initiates the emergency call in supported CS domain CDMA 2000 1xRTT

19.1.3a.4 Method of test

Initial conditions

Same as in 19.1.3.4, except: UE contains ISIM and USIM and CSIM or USIM and CSIM applications on UICC.

The SS is configured:

- with 2 cells: as in TS 36.508
- E-UTRAN cell 1
- 1xRTT cell 19
- Cell 1 power level is set as 'serving cell' and cell 19 power level is set as 'suitable cell'

Related ICS/IXIT Statement(s)

- UE supports IMS emergency services (Yes/No)
- UE supports IPSec ESP confidentiality protection (Yes/No)
- IMS security (Yes/No)
- UE supports emergency call on CS domain 1xRTT (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

Same as in 19.1.3.4

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			User initiates an emergency call	
2-5			Steps defined in annex C.20	EPS emergency bearer context activation and subsequent IMS emergency registration by the UE. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
7	→		INVITE	UE sends INVITE with the first SDP offer indicating all desired medias and codecs the UE supports
6	<-		380 Alternative Service	The SS responds with a 380 Alternative Service response
8	→		ACK	The UE acknowledges the receipt of 380 Alternative Service for INVITE
9			UE performs cell reselection to a cell supporting CS domain (CDMA2000 1XRTT cell) and performs emergency call in CS domain after CDMA registration (if needed)	.
10			CS call is released	

Specific Message Contents

Same as in 19.1.3.4

19.1.3a.5 Test requirements

In step 9, UE initiates a CS emergency call in 1xRTT cell.

19.1.4 Void

19.1.5 Emergency call with emergency registration / Emergency SIP signalling and media in parallel with an other ongoing IM CN subsystem signalling and media

19.1.5.1 Definition and applicability

Test to verify that the UE [IMS registered for non emergency services and ongoing multimedia call] can correctly register to IMS emergency services and initiate an IMS emergency call when UE is registered to IMS non-emergency services of the HPLMN either with ISIM or USIM. The process consists of setting up EPS emergency bearers, sending initial emergency registration to E-CSCF via the P-CSCF discovered, authenticating the user and finally initiating the emergency call. The test case is applicable for IMS security.

19.1.5.2 Conformance requirement

[TS 24.229 clause 5.1.6.1]:

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 and 3GPP TS 23.167 to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

The UE shall determine, whether it is currently attached to its home operator's network (e.g. HPLMN) or to a different network than its home operator's network (e.g. VPLMN) by applying access technology specific procedures described in the access technology specific annexes.

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 [1A] and 3GPP TS 23.167 [4B] to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

The UE shall determine, whether it is currently attached to its home operator's network (e.g. HPLMN) or to a different network than its home operator's network (e.g. VPLMN) by applying access technology specific procedures described in the access technology specific annexes.

[TS 24.229 clause 5.1.6.2]:

When the user initiates an emergency call, if emergency registration is needed (including cases described in subclause 5.1.6.2A), the UE shall perform an emergency registration prior to sending the SIP request related to the emergency call.

...

IP-CAN procedures for emergency registration are defined in 3GPP TS 23.167 [4B] and in each access technology specific annex.

When a UE performs an initial emergency registration the UE shall perform the actions as specified in subclause 5.1.1.2 with the following additions and modifications:

a) the UE shall include a "sos" SIP URI parameter in the Contact header field as described in subclause 7.2A.13, indicating that indicates that this is an emergency registration and that the associated contact address is allowed only for emergency service; and

b) the UE shall populate the From and To header fields of the REGISTER request with:

   - the first entry in the list of public user identities provisioned in the UE;

   - the default public user identity obtained during the normal registration, if the UE is not provisioned with a list of public user identities, but the UE is currently registered to the IM CN subsystem; and

   - the derived temporary public user identity, in all other cases.

When the UE performs an initial emergency registration and whilst this emergency registration is active, the UE shall:

- handle the emergency registration independently from any other ongoing registration to the IM CN subsystem;

- handle any signalling or media related IP-CAN for the purpose of emergency calls independently from any other established IP-CAN for IM CN subsystem related signalling or media; and

- handle all SIP signalling and all media related to the emergency call independently from any other ongoing IM CN subsystem signalling and media.

[TS 24.229 clause 5.1.6.8.3]:

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclause 5.1.2A, 5.1.3 and 5.1.4 with the following additions:

1) the UE shall insert in the INVITE request, a From header field that includes the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration, as described in subclause 4.2;

2) the UE shall include a Request-URI in the INVITE request that contains an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69]. An additional sub-service type can be added if information on the type of emergency service is known;

3) the UE shall insert in the INVITE request, a To header field with:

   - the same emergency service URN as in the Request-URI; or

- if the UE cannot perform local dialstring interpretation for the dialled digits, a dialstring URI representing the dialled digits in accordance with RFC 4967 [103] or a tel URL representing the dialled digits;

NOTE 1: This version of this document does not provide any specified handling of a URI with the dialled digits in accordance with RFC 4967 [103] at an entity within the IM CN subsystem. Behaviour when this is used is therefore not defined.

4) if available to the UE, and if defined for the access type as specified in subclause 7.2A.4, the P-Access-Network-Info header field shall contain a location identifier such as the cell id, line id or the identity of the I-WLAN access node, which is relevant for routeing the IMS emergency call;

NOTE 2: The IMS emergency specification in 3GPP TS 23.167 [4B] describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

5) the UE shall insert in the INVITE request, one or two P-Preferred-Identity header field(s) that include the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration as described in subclause 4.2;

NOTE 3: Providing two P-Preferred-Identity header fields is usually supported by UE acting as enterprise network.

6) void;

7) if the UE has its location information available, then the UE shall include its location information in the INVITE request in the following way:

- if the UE is aware of the URI that points to where the UE's location is stored, include the URI in the Geolocation header field, set the Geolocation-Routing header field to "yes", all in accordance withRFC 6442 [98]; or

- if the geographical location information of the UE is available to the UE, include its geographical location information as PIDF location object in accordance with RFC 4119 [90] and include the location object in a message body with the content type application/pidf+xml in accordance with RFC 6442 [98]. The Geolocation header field is set to a Content ID, and set the Geolocation-Routing header field to "yes", all in accordance with RFC 6442 [98]; and

NOTE 4: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

8) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in RFC 6442 [98] in the INVITE request.

NOTE 5: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

After a successful initial emergency registration, the UE shall apply the procedures as specified in subclause 5.1.2A, 5.1.3 and 5.1.4 with the following additions:

1) the UE shall insert in the INVITE request, a From header field that includes the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration, as described in subclause 4.2;

2) the UE shall include a service URN in the Request-URI of the initial INVITE request in accordance with subclause 5.1.6.8.1;

3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;

4) if available to the UE, and if defined for the access type as specified in subclause 7.2A.4, the P-Access-Network-Info header field shall contain a location identifier such as the cell id, line id or the identity of the I-WLAN access node, which is relevant for routeing the IMS emergency call;

NOTE 2: The IMS emergency specification in 3GPP TS 23.167 [4B] describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

5) the UE shall insert in the INVITE request, one or two P-Preferred-Identity header field(s) that include the public user identity registered via emergency registration or the tel URI associated with the public user identity registered via emergency registration as described in subclause 4.2;

NOTE 2: Providing two P-Preferred-Identity header fields is usually supported by UE acting as enterprise network.

6) void;

7) if the UE has its location information available, or a URI that points to the location information, then the UE shall include a Geolocation header field in the INVITE request in the following way:

- if the UE is aware of the URI that points to where the UE's location is stored, include the URI as the Geolocation header field value, as described in RFC 6442 [89]; or

- if the UE is aware of its location information, include the location information in a PIDF location object, in accordance with RFC 4119 [90], include the location object in a message body with the content type application/pidf+xml, and include a Content ID URL, referring to the message body, as the Geolocation header field value, as described RFC 6442 [89];

8) if the UE includes a Geolocation header field, the UE shall also include a Geolocation-Routing header field with a "yes" header field value, which indicates that the location of the UE can be used by other entities to make routing decisions, as described in RFC 6442 [89]; and

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is not desirable.

9) if the UE has neither geographical location information available, nor a URI that points to the location information, the UE shall not insert a Geolocation header field in the INVITE request.

NOTE 4: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

<discussion see above>

[TS 24.229 annex L.2.2.6]:

Emergency bearers are defined for use in emergency calls in EPS and core network support of these bearers is indicated to the UE in NAS signalling. Where the UE recognises that a call request is an emergency call and the core network supports emergency bearers, the UE shall use these EPS bearer contexts for both signalling and media for emergency calls made using the IM CN subsystem.

...

When activating a EPS bearer context to perform emergency registration, the UE shall request a PDN connection for emergency bearer services as described in 3GPP TS 24.301. The procedures for EPS bearer context activation and P-CSCF discovery, as described in subclause L.2.2.1 of this specification apply accordingly.

In order to find out whether the UE is attached to the home PLMN or to the visited PLMN, the UE shall compare the MCC and MNC values derived from its IMSI with the MCC and MNC of the PLMN the UE is attached to. If the MCC and MNC of the PLMN the UE is attached to do not match with the MCC and MNC derived from the IMSI, then for the purpose of emergency calls in the IM CN subsystem the UE shall consider to be attached to a VPLMN.

NOTE: In this respect an equivalent HPLMN, as defined in 3GPP TS 23.122 will be considered as a visited network.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.6.1, 5.1.6.2, 5.1.6.8.3 and Annex L2.2.6 (release 9)

19.1.5.3 Test purpose

1) To verify that the UE registered for non emergency services and ongoing multimedia call, on initiation of an emergency call, holds the ongoing multimedia call and sends a correctly composed INVITE request for the emergency call setup and will correctly complete the emergency session setup using SDP preconditions, according to 3GPP TS 24.229 [10] clauses 5.1.6.8.3 and 6.1.2.

19.1.5.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step and thereafter executing the generic test procedure in Annex C.21 up to its last step for a multimedia non emergency call.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

Related ICS/IXIT Statement(s)

- UE supports initiating a session (Yes/No)
- UE supports speech (Yes/No)
- Support for IMS Multimedia Telephony (Yes/No)
- UE supports Communication Hold during emergency call (Yes/No)
- UE supports IMS emergency services (Yes/No)
- UE supports IPSec ESP confidentiality protection (Yes/No)
- IMS security (Yes/No)

Test procedure

applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) Ongoing multimedia call is put on hold.
2) IMS emergency call is initiated on the UE.
3)-16) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 15 for EPS emergency bearer context activation, IMS emergency registration and subsequent IMS emergency speech call establishment with PSAP.
17) UE releases the emergency call.
18) Multimedia call is un hold.
19) Multimedia call is released.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			User initiates hold of ongoing call	
2-5	→		Steps defined in annex C.8	Ongoing call is put on hold by UE
6			User initiates an emergency call	
7-15			Steps defined in annex C.20 followed by the steps defined in annex C.22	IMS emergency registration by the UE followed by IMS emergency call setup with PSAP. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
16	→		BYE	The UE releases the emergency call with BYE
17	←		200 OK	The SS sends 200 OK for BYE
18			User initiates un-hold of ongoing call which is on hold	
19	→		INVITE or UPDATE	UE sends INVITE or UPDATE with a SDP offer indicating all medias either as recvonly or sendrecv to release the on hold multimedia call.
20	←		100 Trying	Optional : If the UE sent INVITE in step 28, the SS responds to the INVITE with a 100 Trying provisional response
21	←		200 OK	The SS responds INVITE or UPDATE with 200 OK to indicate that the remote UE can again send media
22	→		ACK	Optional: If the UE sent INVITE in step 28 then UE acknowledges the receipt of 200 OK for INVITE
23	→		BYE	The UE releases the multimedia call
24	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

INVITE (step 1 in procedure in Annex C.22)

Use the default message 'INVITE for MO call setup' in annex A.2.1. with the following conditions:

- A7 'INVITE for creating an emergency session within an emergency registration' shall apply;

19.1.5.5 Test requirements

In steps 7-21, UE performs emergency registration and establishes an emergency call

19.2 Void

19.3 Non-UE detectable emergency call

19.3.1 Non-UE detectable emergency call / IM CN sends a 1xx response / UE geographical location information available

19.3.1.1 Definition and applicability

Test to verify that the UE acts correctly when it receives a 1xx response to an initial request for a dialog from the IM CN, the response containing a P-Asserted-Identity header field set to an emergency number that is recognisable by the UE and the UE sends an UPDATE request with:

- Geolocation header and information if the UE supports this; and
- Contact header set appropriately

19.3.1.2 Conformance requirement

If the UE receives a 1xx or 200 (OK) response to an initial request for a dialog, the response containing a P-Asserted-Identity header field set to an emergency number as specified in 3GPP TS 22.101 [1A], and:

- if a public GRUU value (pub-gruu) has been saved associated with the public user identity, the public GRUU value has not been included in the Contact header field of the initial request for a dialog as specified in RFC 5627 [93];

- if a public GRUU value (pub-gruu) has not been saved and a protected server port was not included in the address in the Contact header field of the initial request for a dialog; or

- if the UE has its geographical location information available and the geographical location information has not been included in the initial request for a dialog; then the UE shall send an UPDATE request according to RFC 3311 [29]; and

  1) if available to the UE, and if defined for the access type as specified in subclause 7.2A.4, the UE shall include in the UPDATE request a P-Access-Network-Info header field and it shall contain a location identifier such as the cell id or the identity of the I-WLAN access node;

  2) if the UE has its geographical location information available, then the UE shall include it in the UPDATE request in the following way:

     I) if the UE is aware of the URI that points to where the UE's location is stored, include the URI in the Geolocation header field and set the "inserted-by" parameter to indicate its hostport, all in accordance with RFC 6442 and set the "inserted-by" parameter to indicate its hostport, all in accordance with draft-ietf-sipcore-loca [98]; or

     II) if the geographical location information of the UE is available to the UE, include its geographical location information as PIDF location object in accordance with RFC 4119 [90] and include the location object in a message body with the content type application/pidf+xml in accordance with RFC 6442 [98]. The Geolocation header field is set to a Content ID and set the "inserted-by" parameter to indicate its hostport, all in accordance withRFC 6442 [98];

  3) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in RFC 6442 [98]; and

  4) if a public GRUU value ("pub-gruu" header field parameter) has been saved associated with the public user identity, then the UE shall insert the public GRUU ("pub-gruu" header field parameter) value in the Contact header field of the UPDATE request as specified in RFC 5627 [93]; otherwise the UE shall include the address in the Contact header field set in accordance with subclause 5.1.6.8.4, item 8.

NOTE 1: The IMS emergency specification in 3GPP TS 23.167 [4B] describes several methods how the UE can get its location information from the access network or from a server. Such methods are not in the scope of this specification.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.6.10

19.3.1.3 Test purpose

To verify that if the UE is not able to detect that an emergency number has been dialled:

- in the event the UE receives a 1xx response to an INVITE request the response containing a P-Asserted-Identity header field set to an emergency number, the UE:

  - If the UE is able to obtain its geolocation and the geographical location information has not been included in the initial request for a dialog; then the UE shall include its geolocation information in the UPDATE message

  - If the UE is not able to obtain its geolocation the UE does not include it in the UPDATE message

  - includes a Contact header in the UPDATE message with the correct contents

19.3.1.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC.

Test environment shall be set up to provide the needed input to the UE, in order for the UE to derive its location, if the UE uses Geolocation header for providing its geographical location. This shall be done by use of the test function Update UE Location Information defined in TS 34.109 [117] or in TS 36.509 [118] depending on the RAT being used in the test case, if supported by the UE according to pc_UpdateUE_LocationInformation. Otherwise, or in addition any other suitable method may also be used.

UE has discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Related ICS/IXIT Statement(s)

- UE supports IMS emergency services (Yes/No)
- Support for speech (Yes/No)
- Support for IMS Multimedia Telephony (Yes/No)
- UE supports IPSec ESP confidentiality protection (Yes/No)
- IMS security (Yes/No)
- obtaining and using GRUUs in the Session Initiation Protocol (SIP) (Yes/No)
- UE uses Geolocation header to provide its geographical location for emergency session setup (Yes/No)
- UE supports test function Update UE Location Information (Yes/No)

Test procedure

1) A non-emergency MO call is initiated up following the generic procedure in Annex C.21.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-12				Steps 1-12 of Annex C.7. The UE initiates a non-emergency call.

INVITE (Step 1)

Use the default message 'INVITE' in annex A.2.1 without options A6 and A7.

183 Session in Progress (Step 3)

Use the default message '183 Session in Progress' in annex A.2.3 with option A5.

UPDATE (Step 6)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Cond	Value/remark	Rel	Reference
Geolocation locationURI	A1	cid-url indicating the Content-Id of the PIDF-LO within the multipart MIME body of INVITE request. (Note that location-by-reference URI is not allowed as the SS does not provide any external storage for location info for the UE to refer.)	Rel-9	RFC 6442 [98]
Geolocation-Routing	A1	'yes'	Rel-9	RFC 6442
Contact pub-gruu addr-spec addr-spec	 A2 A3 A4	 Public GRUU as the SIP URI got from the To header of the REGISTER request, together with the gr parameter with an arbitrary value SIP URI with IP address or FQDN and protected server port of UE SIP URI with IP address or FQDN and unprotected server port of UE		
Content-Type media-type		 *multipart/mixed*		
Message-body		If condition A1 applies, the multipart-mime body shall also contain a PIDF-LO element mapped to the same Content-ID which can be found from the Geolocation header The PIDF-LO shall contain at least the following elements: - One or more "geopriv" elements, each containing: - One "location-info" element describing the location of the UE; and - One "usage-rules" element describing the limitations of the usage of the location info.		RFC 6442 [98]

Condition	Explanation
A1	UE uses Geolocation header to provide its geographical location for emergency session setup
A2	obtaining and using GRUUs in the Session Initiation Protocol (SIP) (A.4/53 3GPP TS 34.229-2 [5])
A3	Not A2 and (IMS security ,A.6a/2 3GPP TS 34.229-2 [5])
A4	Not A2 and (GIBA, A.6a/1 3GPP TS 34.229-2 [5])

180 Ringing (Step 8)

Use the default message '180 Ringing' in annex A.2.6 with option A4.

19.3.1.5 Test requirements

SS must check that in:

- Step 1 the UE sends a non-emergency INVITE with the correct contents
- Step 6 the UE sends the UPDATE message with:
    - the Geolocation header (if supported) set appropriately
    - Conact header set appropriately

19.3.2 Non-UE detectable emergency call / IM CN sends 380 Alternative Service / Non-emergency IMS registration / UTRAN or GERAN

19.3.2.1 Definition and applicability

Test to verify that the UE correctly requests an emergency service on CS domain over UTRAN or GERAN if the UE has received a 380 (Alternative Service) response to an INVITE request.

19.3.2.2 Conformance requirement

In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration and the response containing a 3GPP IM CN subsystem XML body that includes an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.7AA), the UE shall attempt an emergency call as described in subclause 5.1.6.

NOTE 11: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF.

…

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 [1A] and 3GPP TS 23.167 [4B] to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

…

If the UE is connected to more than one domain in which it is possible for the UE to make voice calls, the UE shall attempt an emergency call on the same domain it would use to originate a non-emergency voice call unless serving network policy (based on regulatory requirements and operator needs) requires the UE, including an unauthenticated UE, to attempt the emergency call on a specific domain first.

Reference(s)

3GPP TS 24.229[10], clauses 5.1. 3.1, 5.1.6.1

3GPP TS 22.101[39]: clause 10.1.2

19.3.2.3 Test purpose

To verify that if the UE is not able to detect that an emergency number has been dialled:

- in the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a XML body that includes an <alternative-service> child element with the <type> child element set to "emergency" and the <action> element is not set to "emergency-registration", the UE:
- send an ACK request to the P-CSCF as per normal SIP procedures;
- attempt an emergency call setup via CS domain over UTRAN or GERAN according to the procedures described in 3GPP TS 24.008 [12], only if the P-Asserted-Identity header field with a value equal to the value of the SIP URI of the P-CSCF received in the Path header field during registration.

19.3.2.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. UE has activated EPS bearers, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

The SS is configured:

- with 2 cells: as in TS 36.508
- E-UTRAN cell 1
- if px_RATComb_Tested = EUTRA_UTRA, cell 5
- if px_RATComb_Tested = EUTRA_GERAN, GERAN cell 24
- Cell 1 power level is set as 'serving cell' and cell 24/cell 5 power level is set as 'suitable cell'

Related ICS/IXIT Statement(s)

- IMS security (Yes/No)
- GIBA (Yes/No)
- UE supports Emergency speech call (Yes/No)
- UE supports emergency speech call on CS domain (UTRAN/GERAN) (Yes/No)
- Network supports UTRAN or GERAN (px_RATComb_Tested)

Note: Setting px_RATComb_Tested = EUTRA_Only is not allowed.

Test procedure

1-2) MO call is initiated on the UE by dialling a non emergency number.

3) SS responds to the INVITE request with a 380 Alternative Service.

4) SS waits for the UE to send an ACK to acknowledge receipt of the 380 Alternative Service.

5) SS waits for an emergency call setup according to the procedures described in 3GPP TS 24.008 [12].

6) Having reached the active state, the call is cleared by the SS.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1				MO call is initiated on the UE by dialling a 'non emergency' number.
2	→		INVITE	UE sends INVITE. Request-URI of the INVITE request matches with the 'non emergency' number dialled.
3	←		380 Alternative Service	The SS responds with a 380 Alternative Service
4	→		ACK	The UE acknowledges the receipt of 380 response for INVITE and starts the emergency call in CS domain
5				SS waits for an emergency call setup. according to the procedures described in 3GPP TS 24.008[12].
6				Having reached the active state, the call is cleared by the SS

NOTE: The default messages contents in annex A are used with condition 'IMS security ' or 'GIBA' when applicable.

Specific Message Contents

ATTACH ACCEPT (preamble)

Use the default message as in TS 36.508 [94] sub-clause Table 4.7.2-1 except the following change:

Information Element	Value/remark	Comment
EPS network feature support	'0000 0001'B	IMS voice over PS session in S1 mode supported emergency bearer services in S1 mode not supported

INVITE (Step 2)

Use the default message 'INVITE' in annex A.2.1 for MO Call' in annex A.2.1 with the following exceptions:

Header/param	Value/remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o=-* (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=*(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] Time description: - *t=* (start-time) (stop-time) Media description: - *m=audio* (transport port) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Note 1: At least one "c=" field shall be present. Note 2: AMR codec shall be present

380 Alternative Service (Step 3)

Use the default message '380 Alternative Service' in annex A.4.1.

ACK (Step 4)

Use the default message "ACK" in annex A.2.7

19.3.2.5 Test requirements

Check that the UE sends all the requests over the security associations set up during registration, in accordance to 3GPP TS 24.229 [10], clause 5.1.1.5.1.

Step 2: the UE sends an INVITE message with correct content.

Step 5, 6: Check that the emergency call on the CS domain UTRAN or GERAN is successfully established according to the procedures described in 3GPP TS 24.008 [12].

19.3.2a Non-UE detectable emergency call / IM CN sends 380 Alternative Service / Non-emergency IMS registration / CDMA 2000 1xRTT

19.3.2a.1 Definition and applicability

Same as in 19.3.2.1, except: UE correctly requests an emergency service on CS domain over CDMA 2000 1xRTT.

19.3.2a.2 Conformance requirement

Same Conformance requirement as in clause 19.3.2.2

19.3.2a.3 Test purpose

To verify that if the UE is not able to detect that an emergency number has been dialled:

- in the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a XML body that includes an <alternative-service> child element with the <type> child element set to "emergency" and the <action> element is not set to "emergency-registration", the UE:

- send an ACK request to the P-CSCF as per normal SIP procedures;

- attempt an emergency call setup via CS domain CDMA 2000 1xRTT according to the procedures described in 3GPP2 TS C.S0005-E[112], only if the P-Asserted-Identity header field with a value equal to the value of the SIP URI of the P-CSCF received in the Path header field during registration.

19.3.2a.4 Method of test

Initial conditions

Same as in 19.3.2.4, except: UE contains ISIM and USIM and CSIM or USIM and CSIM applications on UICC.

The SS is configured:

- with 2 cells: as in TS 36.508

- E-UTRAN cell 1

- 1xRTT cell 19

- Cell 1 power level is set as 'serving cell' cell 19 power level is set as 'suitable cell'

Related ICS/IXIT Statement(s)

- IMS security (Yes/No)

- GIBA (Yes/No)

- UE supports Emergency speech call (Yes/No)

- UE supports emergency speech call over 1xRTT (Yes/No)

Test procedure

Same as in 19.3.2.4 except step 5:

5) SS waits for an emergency call setup according to the procedures described in 3GPP2 TS C.S0005-E[112].

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1				MO call is initiated on the UE by dialling a 'non emergency' number.
2	→		INVITE	UE sends INVITE. Request-URI of the INVITE request matches with the 'non emergency' number dialled.
3	←		380 Alternative Service	The SS responds with a 380 Alternative Service
4	→		ACK	The UE acknowledges the receipt of 380 response for INVITE and starts the emergency call in CS domain
5				SS waits for an emergency call setup. according to the procedures described in 3GPP2 TS C.S0005-E[112] .
6				Having reached the active state, the call is cleared by the SS

NOTE: The default messages contents in annex A are used with condition 'IMS security ' or 'GIBA ' when applicable.

Specific Message Contents

Same as in 19.3.2.4

19.3.2a.5 Test requirements

Same as 19.3.2.5.

Except Steps 5, 6: SS must check that the emergency call on the CS domain CDMA 2000 1xRTT is successfully established according to the procedures described in 3GPP TS 24.008 [12].

19.3.3 Non-UE detectable emergency call / IM CN sends 380 Alternative Service / Emergency IMS registration

19.3.3.1 Definition and applicability

To verify that In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration and the response containing a 3GPP IM CN subsystem XML body that includes an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.7AA), the UE shall attempt an emergency call as described in subclause 5.1.6.

19.3.3.2 Conformance requirement

In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration and the response containing a 3GPP IM CN subsystem XML body that includes an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.7AA), the UE shall attempt an emergency call as described in subclause 5.1.6.

NOTE 11: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.3.1.

19.3.3.3 Test purpose

To verify that In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration and the response containing a 3GPP IM CN subsystem XML body that includes an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.7AA), the UE shall attempt an emergency call as described in subclause 5.1.6.

19.3.3.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. UE has activated EPS bearers, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Related ICS/IXIT Statement(s)

- UE supports IMS emergency services (Yes/No)
- UE uses Geolocation header to provide its geographical location for emergency session setup (Yes/No)
- UE supports IPSec ESP confidentiality protection (Yes/No)
- IMS security (Yes/No)
- GIBA (Yes/No)

Test procedure

1-2) MO call is initiated on the UE by dialling a non emergency number.

3) SS responds to the INVITE request with a 380 Alternative Service.

4) SS waits for the UE to send an ACK to acknowledge receipt of the 380 Alternative Service.

5-19) SS waits for an IMS emergency registration and call setup.

20-21) Having reached the active state, the call is cleared by the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1				MO call is initiated on the UE by dialling a 'non emergency' number.
2	→		INVITE	UE sends INVITE. Request-URI of the INVITE request matches with the 'non emergency' number dialled.
3	←		380 Alternative Service	The SS responds with a 380 Alternative Service
4	→		ACK	The UE acknowledges the receipt of 380 response for INVITE.
5-19			Steps defined in annex C.20 followed by the steps defined in annex C.22	IMS emergency registration by the UE followed by IMS emergency call setup with PSAP. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
20	→		BYE	The UE releases the call with BYE
21	←		200 OK	The SS sends 200 OK for BYE

NOTE: The default messages contents in annex A are used with condition 'IMS security '.

Specific Message Contents

INVITE (Step 2 of Annex C.21)

Use the default message 'INVITE' in annex A.2.1. for MO Call' in annex A.2.1 with the following exceptions:

Header/param	Value/remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o=-* (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=*(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] Time description: - *t=* (start-time) (stop-time) Media description: - *m=audio* (transport port) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Note 1: At least one "c=" field shall be present. Note 2: AMR codec shall be present

380 Alternative Service (Step 3)

Use the default message '380 Alternative Service' in annex A.4.1 with the following exception.

Header/param	Value/remark	Rel	Reference
Message-body	*<?xml version="1.0"?>* *<ims-3gpp version="1">* *<alternative-service>* *<type>emergency</type>* *<reason/>* *<action>*emergency-registration</action> *</alternative-service>* *</ims-3gpp>*		

ACK (Step 4)

Use the default message "ACK" in annex A.2.7

INVITE (step 1 of Annex C.22)

Use the default message 'INVITE for MO call setup' in annex A.2.1. with the following conditions:

- A7 'INVITE for creating an emergency session within an emergency registration' shall apply; and
- A8 'UE uses Geolocation header to provide its geographical location for emergency session setup, has obtained its location and is setting up an emergency session ' shall apply if the UE uses Geolocation header to provide its geographical location for emergency session setup.

180 Ringing for INVITE (step 3 of Annex C.22)

Use the default message '180 Ringing for INVITE' in annex A.2.6 The condition A4 '180 sent by the SS when setting up an emergency call' shall apply.

200 OK for INVITE (step 4 of Annex C.22)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1. The condition A6 'Response sent by SS for INVITE for emergency call' shall apply

BYE (Step 20)

Use the default message 'BYE' in annex A.2.8.

19.3.3.5 Test requirements

Steps 5-19: the UE sets up emergency call correctly.

19.3.4 Non-UE detectable emergency call / IM CN sends 380 with an Alternative Service / Previous emergency IMS registration not expired

19.3.4.1 Definition and applicability

To verify that In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration and the response containing a 3GPP IM CN subsystem XML body that includes an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.7AA), the UE shall attempt an emergency call as described in subclause 5.1.6.

19.3.4.2 Conformance requirement

In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration and the response containing a 3GPP IM CN subsystem XML body that includes an <ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.7AA), the UE shall attempt an emergency call as described in subclause 5.1.6.

NOTE 11: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF.

…

The UE shall perform a new initial emergency registration, as specified in subclause 5.1.6.2, if the UE determines that:

- it has previously performed an emergency registration which has not yet expired; and
- it has obtained an IP address from the serving IP-CAN, as specified in subclause 9.2.1, different than the IP address used for the emergency registration.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.3.1, 5.1.6.2A.

19.3.4.3 Test purpose

To verify that In the event the UE receives a 380 (Alternative Service) response to an INVITE request the response containing a P-Asserted-Identity header field with a value equal to the value of the last entry on the Path header field value received during registration and the response containing a 3GPP IM CN subsystem XML body that includes an

<ims-3gpp> element, including a version attribute, with an <alternative-service> child element with the <type> child element set to "emergency" (see table 7.7AA), the UE shall attempt an emergency call as described in subclause 5.1.6.

19.3.4.4 Method of test

Initial conditions

UE contains ISIM and USIM applications or only USIM application on UICC. UE has activated EPS bearers, discovered P-CSCF and registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

SS is configured with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) configured on the UICC card equipped into the UE. SS has performed AKAv1-MD5 authentication with the UE and accepted the registration.

Related ICS/IXIT Statement(s)

- UE supports IMS emergency services (Yes/No)
- UE uses Geolocation header to provide its geographical location for emergency session setup (Yes/No)
- UE supports IPSec ESP confidentiality protection (Yes/No)
- IMS security (Yes/No)
- GIBA (Yes/No)

Test procedure

1-15) Emergency registration followed by an emergency call set-up

16-17) The emergency call is terminated by the UE

18) MO call is initiated on the UE by dialling a non emergency number.

19) SS waits the UE to send an INVITE request with Request-URI that matches the non emergency number dialled.

20) SS responds to the INVITE request with a 380 Alternative Service.

21) SS waits for the UE to send an ACK to acknowledge receipt of the 380 Alternative Service.

22-37) SS waits for an IMS emergency registration and a call setup.

38-39) Having reached the active state, the call is cleared by the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-15			Steps defined in annex C.20 followed by the steps defined in annex C.22	IMS emergency registration by the UE followed by IMS emergency call setup with PSAP. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
16	→		BYE	The UE releases the call with BYE
17	←		200 OK	The SS sends 200 OK for BYE
18				MO call is initiated on the UE by dialling a 'non emergency' number.
19	→		INVITE	UE sends INVITE. Request-URI of the INVITE request matches with the 'non emergency' number dialled.
20	←		380 Alternative Service	The SS responds with a 380 Alternative Service
21	→		ACK	The UE acknowledges the receipt of 380 response for INVITE.
22-25			Steps defined in annex C.20 for emergency registration	Optional procedure: IMS emergency registration. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
26-37			Steps defined in annex C.22	IMS emergency call setup with PSAP. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
38	→		BYE	The UE releases the call with BYE
39	←		200 OK	The SS sends 200 OK for BYE

NOTE: The default messages contents in annex A are used with condition 'IMS security '.

Specific Message Contents

INVITE (Step 19)

Use the default message 'INVITE' in annex A.2.1. for MO Call' in annex A.2.1 with the following exceptions:

Header/param	Value/remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o=*- (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=*(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] Time description: - *t=* (start-time) (stop-time) Media description: - *m=audio* (transport port) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Note 1: At least one "c=" field shall be present. Note 2: AMR codec shall be present

380 Alternative Service (Step 20)

Use the default message '380 Alternative Service' in annex A.4.1 with the following exception.

Header/param	Value/remark	Rel	Reference
Message-body	*<?xml version="1.0"?>* *<ims-3gpp version="1">* *<alternative-service>* *<type>emergency</type>* *<reason/>* <action>emergency-registration</action> *</alternative-service>* *</ims-3gpp>*		

ACK (Step 21)

Use the default message "ACK" in annex A.2.7

INVITE (step 1 of Annex C.22)

Use the default message 'INVITE for MO call setup' in annex A.2.1. with the following conditions:

- A7 'INVITE for creating an emergency session within an emergency registration' shall apply; and
- A8 'UE uses Geolocation header to provide its geographical location for emergency session setup, has obtained its location and is setting up an emergency session ' shall apply if the UE uses Geolocation header to provide its geographical location for emergency session setup.

180 Ringing for INVITE (step 3 of Annex C.22)

Use the default message '180 Ringing for INVITE' in annex A.2.6. The condition A4 '180 sent by the SS when setting up an emergency call' shall apply.

200 OK for INVITE (step 4 of Annex C.22)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1. The condition A6 'Response sent by SS for INVITE for emergency call' shall apply

BYE (Steps 16, 38)

Use the default message 'BYE' in annex A.2.8.

19.3.4.5 Test requirements

Steps 26-37: the UE sets up emergency call correctly.

19.4 Emergency session set-up in case of no registration

19.4.1 Emergency call without emergency registration / EPS / UE does not contain an ISIM or USIM

19.4.1.1 Definition and applicability

Test to verify that the UE can initiate an IMS emergency call when the UE does not contain ISIM or USIM. The test case is applicable for IMS security.

19.4.1.2 Conformance requirement

Reference(s)

3GPP TS 24.229[10], clauses 5.1.6.1 and 5.1.6.8.2.

[TS 24.229 clause 5.1.6.1]

If the IM CN subsystem is selected and the UE has no credentials the UE can make an emergency call without being registered. The UE shall attempt an emergency call as described in subclause 5.1.6.8.2.

If the IM CN subsystem is selected and the UE has no credentials the UE can make an emergency call without being registered. The UE shall attempt an emergency call as described in subclause 5.1.6.8.2.

[TS 24.229 clause 5.1.6.8.2]

Prior to establishing an emergency session for an unregistered user, the UE shall acquire a local IP address, discover a P-CSCF, and establish an IP-CAN bearer that can be used for SIP signalling. The UE shall send only the initial INVITE requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, the UE shall send the initial INVITE request to the SIP default port values as specified in RFC 3261.

The UE shall apply the procedures as specified in subclause 5.1.2A.1 and subclause 5.1.3 with the following additions:

1) the UE shall set the From header field of the INVITE request to "Anonymous" as specified in RFC 3261;

2) the UE shall include a Request-URI in the initial INVITE request that contains an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031. An additional sub-service type can be added if information on the type of emergency service is known;

NOTE 1: Other specifications make provision for emergency service identifiers that are not specifically the emergency service URN, to be recognised in the UE. Emergency service identifiers which the UE does not detect will be treated as a normal call by the UE.

3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;

4) if available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall include in the P-Access-Network-Info header field in any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request. The UE shall populate the P-Access-Network-Info header field with the current point of attachment to the IP-CAN as specified for the access network technology (see subclause 7.2A.4). The P-Access-Network-Info header field contains the location identifier such as the cell id, the line id or the identity of the I-WLAN access node, which is relevant for routeing the emergency call;

5) if defined by the access technology specific annex, the UE shall populate the P-Preferred-Identity header field in the INVITE request with an equipment identifier as a SIP URI. The special details of the equipment identifier to use depends on the IP-CAN;

6) a Contact header field set to include SIP URI that contains in the hostport parameter the IP address of the UE and an unprotected port where the UE will receive incoming requests belonging to this dialog. The UE shall also include a "sip.instance" media feature tag containing Instance ID as described in RFC 5626. The UE shall not include either the public or temporary GRUU in the Contact header field;

7) a Via header field set to include the IP address of the UE in the sent-by field and for the UDP the unprotected server port value where the UE will receive response to the emergency request, while for the TCP, the response is received on the TCP connection on which the emergency request was sent. For the UDP, the UE shall also include "rport" header field parameter with no value in the top Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with, and during the lifetime of, the emergency session, as described in draft-ietf-sipcore-keep;

NOTE 2: The UE inserts the same IP address and port number into the Contact header field and the Via header field, and sends all IP packets to the P-CSCF from this IP address and port number.

8) if the UE has its location information available, the UE shall include the location information in the INVITE request in the following way:

   - if the UE is aware of the URI that points to where the UE's location is stored, include the URI in the Geolocation header field, in accordance with RFC 6442 [98]; or

- if the geographical location information of the UE is available to the UE, include its geographical location information as PIDF location object in accordance with RFC 4119 and include the location object in a message body with the content type application/pidf+xml in accordance with RFC 6442 [98]. The Geolocation header field is set to a Content ID, in accordance with RFC 6442 [98]; and

9) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in RFC 6442 [98] in the INVITE request.

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is inapplicable in this area.

NOTE 5: During the dialog, the points of attachment to the IP-CAN of the UE can change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header field in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header field value for all new dialogs. The UE shall build a Route header field value containing only the P-CSCF URI (containing the unprotected port number and the IP address or the FQDN learnt through the P-CSCF discovery procedures).

19.4.1.3 Test purpose

1) To verify that the UE is able to request activation of EPS emergency bearer contexts, according to 3GPP TS 24.229 [10] 5.1.6.1; and

2) To verify that the UE sends a correctly composed SIP INVITE request for the emergency call setup and will correctly complete the emergency session setup, according to 3GPP TS 24.229 [10] clauses 5.1.6.8.2 and 6.1.2.

19.4.1.4 Method of test

Initial conditions

The UE is Switched OFF and contains no ISIM or USIM.

Related ICS/IXIT Statement(s)

- UE supports IMS emergency services (Yes/No)
- IMS security (Yes/No)
- obtaining and using GRUUs in the Session Initiation Protocol (SIP) (Yes/No)
- UE uses Geolocation header to provide its geographical location for emergency session setup (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-19) UE executes the procedures described in TS 36.508 [94] table 4.5A.5.3-1 steps 1 to 19 for EPS emergency bearer context activation and subsequent IMS emergency speech call.

Expected sequence:

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-5			Steps defined in annex C.22	Generic test procedure for setting up emergency speech call. Referred from 36.508 [94] table 4.5A.5.3-1 for a UE with E-UTRA support.
6	→		BYE	UE release the call.
7	←		200 OK	SS responds.

Specific Message Contents

INVITE (Step 1)

Use the default message 'INVITE for MO call setup' in annex A.2.1. with the following conditions:

- A6 'INVITE for creating an emergency session in case of no registration' shall apply; and
- A8 'UE uses Geolocation header to provide its geographical location for emergency session setup, has obtained its location and is setting up an emergency session ' shall apply if the UE uses Geolocation header to provide its geographical location for emergency session setup.

BYE (Step 6)

Use the default message 'BYE' in annex A.2.8.

200 OK (Step 7)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

19.4.1.5 Test requirements

The UE shall send requests and responses as described in clause 19.4.1.4.

19.4.2 Emergency call without emergency registration / EPS / UE contains an ISIM or USIM / UE is in state EMM-REGISTERED.LIMITED-SERVICE

19.4.2.1 Definition and applicability

Test to verify that the UE with ISIM or USIM and in state EMM-REGISTERED.LIMITED-SERVICE, establishes an emergency call if emergency call is initiated, The process consists of setting the emergency call. without any IMS (non emergency or emergency) registration.

19.4.2.2 Conformance requirement

[TS 24.229 clause L.2.2.6]:

Emergency bearers are defined for use in emergency calls in EPS and core network support of these bearers is indicated to the UE in NAS signalling. Where the UE recognises that a call request is an emergency call and the core network supports emergency bearers, the UE shall use these EPS bearer contexts for both signalling and media for emergency calls made using the IM CN subsystem.

Some jurisdictions allow emergency calls to be made when the UE does not contain an ISIM or USIM, or where the credentials are not accepted. Additionally where the UE is in state EMM-REGISTERED.LIMITED-SERVICE and EMM-REGISTERED.PLMN-SEARCH, a normal ATTACH has been attempted and it can also be assumed that a registration in the IM CN subsystem will also fail. In such cases, the procedures for emergency calls without registration apply, as defined in subclause 5.1.6.8.2.

[TS 24.229 clause 5.1.6.8.2]:

When establishing an emergency session for an unregistered user, the UE is allowed to receive responses to emergency requests and requests inside an established emergency session on the unprotected ports. The UE shall reject or silently discard all other messages not arriving on a protected port. Additionally, the UE shall transmit signalling packets pertaining to the emergency session from the same IP address and unprotected port on which it expects to receive signalling packets containing the responses to emergency requests and the requests inside the established emergency session.

Prior to establishing an emergency session for an unregistered user, the UE shall acquire a local IP address, discover a P-CSCF, and establish an IP-CAN bearer that can be used for SIP signalling. The UE shall send only the initial INVITE requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any

specific port information during the P-CSCF discovery procedure, the UE shall send the initial INVITE request to the SIP default port values as specified in RFC 3261 [26].

The UE shall apply the procedures as specified in subclause 5.1.2A.1 and subclause 5.1.3 with the following additions:

1) the UE shall set the From header field of the INVITE request to "Anonymous" as specified in RFC 3261 [26];

2) the UE shall include a Request-URI in the initial INVITE request that contains an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69]. An additional sub-service type can be added if information on the type of emergency service is known;

NOTE 1: Other specifications make provision for emergency service identifiers that are not specifically the emergency service URN, to be recognised in the UE. Emergency service identifiers which the UE does not detect will be treated as a normal call by the UE.

3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;

4) if available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall include in the P-Access-Network-Info header field in any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request. The UE shall populate the P-Access-Network-Info header field with the current point of attachment to the IP-CAN as specified for the access network technology (see subclause 7.2A.4). The P-Access-Network-Info header field contains the location identifier such as the cell id, the line id or the identity of the I-WLAN access node, which is relevant for routeing the emergency call;

5) if defined by the access technology specific annex, the UE shall populate the P-Preferred-Identity header field in the INVITE request with an equipment identifier as a SIP URI. The special details of the equipment identifier to use depends on the IP-CAN;

6) a Contact header field set to include SIP URI that contains in the hostport parameter the IP address of the UE and an unprotected port where the UE will receive incoming requests belonging to this dialog. The UE shall also include a "sip.instance" media feature tag containing Instance ID as described in RFC 5626 [92]. The UE shall not include either the public or temporary GRUU in the Contact header field;

7) a Via header field set to include the IP address of the UE in the sent-by field and for the UDP the unprotected server port value where the UE will receive response to the emergency request, while for the TCP, the response is received on the TCP connection on which the emergency request was sent. For the UDP, the UE shall also include "rport" header field parameter with no value in the top Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with, and during the lifetime of, the emergency session, as described in draft-ietf-sipcore-keep [143];

NOTE 2: The UE inserts the same IP address and port number into the Contact header field and the Via header field, and sends all IP packets to the P-CSCF from this IP address and port number.

8) if the UE has its location information available, the UE shall include the location information in the INVITE request in the following way:

   - if the UE is aware of the URI that points to where the UE's location is stored, include the URI in the Geolocation header field, in accordance withRFC 6442 [98]; or

   - if the geographical location information of the UE is available to the UE, include its geographical location information as PIDF location object in accordance with RFC 4119 [90] and include the location object in a message body with the content type application/pidf+xml in accordance with RFC 6442 [98]. The Geolocation header field is set to a Content ID, in accordance with RFC 6442 [98]; and

9) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in RFC 6442 [98] in the INVITE request.

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is inapplicable in this area.

NOTE 4: During the dialog, the points of attachment to the IP-CAN of the UE can change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header field in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header field value for all new dialogs. The UE shall build a Route header field value containing only the P-CSCF URI (containing the unprotected port number and the IP address or the FQDN learnt through the P-CSCF discovery procedures).

When a SIP transaction times out, i.e. timer B, timer F or timer H expires at the UE, the UE may behave as if timer F expired, as described in subclause 5.1.1.4.

NOTE 5: It is an implementation option whether these actions are also triggered by other means.

NOTE 6: A number of header fields can reveal information about the identity of the user. Where privacy is required, implementers should also give consideration to other header fields that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of header fields.

NOTE 7: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

If the response for the initial INVITE request indicates that the UE is behind NAT, and the INVITE request was sent over TCP connection, the UE shall keep the TCP connection during the entire duration of the emergency session. In this case the UE will receive all responses to the emergency requests and the requests inside the established emergency session over this TCP connection.

If the Via header field of any provisional response, or of the final 200 (OK) response, for the initial INVITE request contains a "keep" header field parameter with a value, unless the UE detects that it is not behind a NAT, the UE shall start to send keep-alives associated with the session towards the P-CSCF, as described in draft-ietf-sipcore-keep [143].

Reference(s)

3GPP TS 24.229[10], clauses 5.1.6.8.2 and Annex L2.2.6 (release 9)

19.4.2.3 Test purpose

1) To verify that the UE in state EMM-REGISTERED.LIMITED-SERVICE ,not registered for non emergency services , on initiation of an emergency call, performs EMM emergency registration to acquire a local IP address, discover a P-CSCF, and establish an IP-CAN bearer that can be used for SIP signalling and then composed INVITE request for the emergency call setup and will correctly complete the emergency session setup using SDP preconditions, according to 3GPP TS 24.229 [10] clauses 5.1.6.8.2 and 6.1.2.

19.4.2.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is in state EMM-REGISTERED.LIMITED-SERVICE[FFS: can be achieved by rejecting the Tracking Area Update procedure with cause #15, No suitable cells in tracking area; UE is initially registered in cell A and made to select cell B. The Tracking area update procedure is rejected with cause #15 in cell B], not registered for IMS services,

SS is configured with the IMSI within the USIM application, the home domain name, SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS supports EMM emergency attach procedure and emergency bearers.

The SS configures two cells as below:

EUTRA cell A and Cell B as in TS 36.508

Related ICS/IXIT Statement(s)

- UE supports initiating a session (Yes/No)
- UE supports IMS emergency services (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

- the IMS emergency call is initiated on the UE.
- UE executes the procedures described in TS 36.508 [94] table 4.5A.5.3-1 steps 1 to 19 for EMM Emergency registration, EPS emergency bearer context activation, IMS emergency speech call establishment with PSAP.
-

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			User initiates an emergency call	
2-6			Steps defined in annex C.22	Generic test procedure for setting up emergency speech call. Referred from 36.508 [94] table 4.5A.5.3-1 for a UE with E-UTRA support.
7	→		BYE	The UE releases the emergency call
8	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

INVITE (step 1 of procedure in annex C.22)

Use the default message 'INVITE for MO call setup' in annex A.2.1. with the following conditions:

- A7 'INVITE for creating an emergency session within an emergency registration' shall apply;

19.4.2.5 Test requirements

In steps 2-6, UE establishes an emergency call.

19.4.3 Emergency call without emergency registration / GPRS / UE does not contain an ISIM or USIM / UE is in state GMM-NO USIM

19.4.3.1 Definition and applicability

Test to verify that the UE with ISIM or USIM and in state GMM-DEREGISTERED.substate no IMSI, establishes an emergency call if emergency call is initiated, The process consists of setting the emergency call. without any IMS (non emergency or emergency) registration.

19.4.3.2 Conformance requirement

[TS 24.229 clause 5.1.1.1B.1]:

In case the UE contains neither an ISIM nor a USIM, but IMC is present the UE shall use preconfigured parameters in the IMC to initiate the registration to the IM CN subsystem and for authentication.

The following IMS parameters are assumed to be available to the UE:

- a private user identity;
- a public user identity; and
- a home network domain name to address the SIP REGISTER request to.

These parameters may not necessarily reside in a UICC.

The first public user identity in the list stored in the IMC is used in emergency registration requests.

[TS 24.229 clause B.2.2.6]:

Emergency bearers are defined for use in emergency calls in GPRS and core network support of these bearers is indicated to the UE in NAS signalling. Where the UE recognises that a call request is an emergency call and the core network supports emergency bearers, the UE shall use these bearers for both signalling and media on emergency calls made using the IM CN subsystem.

Some jurisdictions allow emergency calls to be made when the UE does not contain an ISIM or USIM, or where the credentials are not accepted. Additionally where the UE is in state GMM-REGISTERED.LIMITED-SERVICE and GMM-REGISTERED.PLMN-SEARCH, a normal ATTACH has been attempted and it can also be assumed that a registration in the IM CN subsystem will also fail. In such cases, the procedures for emergency calls without registration apply, as defined in subclause 5.1.6.8.2.

When activating a PDP context to perform emergency registration, the UE shall request a PDP context for emergency bearer services as defined in 3GPP TS 24.008 [8]. The procedures for PDP context activation and P-CSCF discovery, as described in subclause B.2.2.1 of this specification apply accordingly.

In order to find out whether the UE is attached to the home PLMN or to the visited PLMN, the UE shall compare the MCC and MNC values derived from its IMSI with the MCC and MNC of the PLMN the UE is attached to. If the MCC and MNC of the PLMN the UE is attached to do not match with the MCC and MNC derived from the IMSI, then for the purpose of emergency calls in the IM CN subsystem the UE shall consider to be attached to a VPLMN.

NOTE: In this respect an equivalent HPLMN, as defined in 3GPP TS 23.122 [4C] will be considered as a visited network.

[TS 24.229 clause 5.1.6.8.2]:

When establishing an emergency session for an unregistered user, the UE is allowed to receive responses to emergency requests and requests inside an established emergency session on the unprotected ports. The UE shall reject or silently discard all other messages not arriving on a protected port. Additionally, the UE shall transmit signalling packets pertaining to the emergency session from the same IP address and unprotected port on which it expects to receive signalling packets containing the responses to emergency requests and the requests inside the established emergency session.

Prior to establishing an emergency session for an unregistered user, the UE shall acquire a local IP address, discover a P-CSCF, and establish an IP-CAN bearer that can be used for SIP signalling. The UE shall send only the initial INVITE requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, the UE shall send the initial INVITE request to the SIP default port values as specified in RFC 3261 [26].

The UE shall apply the procedures as specified in subclause 5.1.2A.1 and subclause 5.1.3 with the following additions:

1) the UE shall set the From header field of the INVITE request to "Anonymous" as specified in RFC 3261 [26];

2) the UE shall include a Request-URI in the initial INVITE request that contains an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69]. An additional sub-service type can be added if information on the type of emergency service is known;

NOTE 1: Other specifications make provision for emergency service identifiers that are not specifically the emergency service URN, to be recognised in the UE. Emergency service identifiers which the UE does not detect will be treated as a normal call by the UE.

3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;

4) if available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall include in the P-Access-Network-Info header field in any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request. The UE shall populate the P-Access-Network-Info header field with the current point of attachment to the IP-CAN as specified for the access network technology (see subclause 7.2A.4). The P-Access-Network-Info header field contains the location identifier such as the cell id, the line id or the identity of the I-WLAN access node, which is relevant for routeing the emergency call;

5) if defined by the access technology specific annex, the UE shall populate the P-Preferred-Identity header field in the INVITE request with an equipment identifier as a SIP URI. The special details of the equipment identifier to use depends on the IP-CAN;

6) a Contact header field set to include SIP URI that contains in the hostport parameter the IP address of the UE and an unprotected port where the UE will receive incoming requests belonging to this dialog. The UE shall also include a "sip.instance" media feature tag containing Instance ID as described in RFC 5626 [92]. The UE shall not include either the public or temporary GRUU in the Contact header field;

7) a Via header field set to include the IP address of the UE in the sent-by field and for the UDP the unprotected server port value where the UE will receive response to the emergency request, while for the TCP, the response is received on the TCP connection on which the emergency request was sent. For the UDP, the UE shall also include "rport" header field parameter with no value in the top Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with, and during the lifetime of, the emergency session, as described in draft-ietf-sipcore-keep [143];

NOTE 2: The UE inserts the same IP address and port number into the Contact header field and the Via header field, and sends all IP packets to the P-CSCF from this IP address and port number.

8) if the UE has its location information available, the UE shall include the location information in the INVITE request in the following way:

- if the UE is aware of the URI that points to where the UE's location is stored, include the URI in the Geolocation header field, in accordance withRFC 6442 [98]; or

- if the geographical location information of the UE is available to the UE, include its geographical location information as PIDF location object in accordance with RFC 4119 [90] and include the location object in a message body with the content type application/pidf+xml in accordance with RFC 6442 [98]. The Geolocation header field is set to a Content ID, in accordance with RFC 6442 [98]; and

9) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in RFC 6442 [98] in the INVITE request.

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is inapplicable in this area.

NOTE 4: During the dialog, the points of attachment to the IP-CAN of the UE can change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header field in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header field value for all new dialogs. The UE shall build a Route header field value containing only the P-CSCF URI (containing the unprotected port number and the IP address or the FQDN learnt through the P-CSCF discovery procedures).

When a SIP transaction times out, i.e. timer B, timer F or timer H expires at the UE, the UE may behave as if timer F expired, as described in subclause 5.1.1.4.

NOTE 5: It is an implementation option whether these actions are also triggered by other means.

NOTE 6: A number of header fields can reveal information about the identity of the user. Where privacy is required, implementers should also give consideration to other header fields that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of header fields.

NOTE 7: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

If the response for the initial INVITE request indicates that the UE is behind NAT, and the INVITE request was sent over TCP connection, the UE shall keep the TCP connection during the entire duration of the emergency session. In this case the UE will receive all responses to the emergency requests and the requests inside the established emergency session over this TCP connection.

If the Via header field of any provisional response, or of the final 200 (OK) response, for the initial INVITE request contains a "keep" header field parameter with a value, unless the UE detects that it is not behind a NAT, the UE shall start to send keep-alives associated with the session towards the P-CSCF, as described in draft-ietf-sipcore-keep [143].

Reference(s)

3GPP TS 24.229[10], clauses 5.1.1.1B.1, 5.1.6.8.2 and Annex B.2.2.6 (release 9)

19.4.3.3 Test purpose

1) To verify that the UE no USIM or ISIM ,not registered for non emergency services , on initiation of an emergency call, performs GMM emergency attach to acquire a local IP address, discover a P-CSCF, and establish an IP-CAN bearer that can be used for SIP signalling and then composed INVITE request for the emergency call setup and will correctly complete the emergency session setup using SDP preconditions, according to 3GPP TS 24.229 [10] clauses 5.1.6.8.2 and 6.1.2.

19.4.3.4 Method of test

Initial conditions

The UE contains neither USIM nor ISIM. UE is in state GMM-DEREGISTERED, no IMSI; Not registered to IMS services,

SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS supports GMM emergency attach procedure and PDP context establishment for emergency bearers.

The SS configures one cell as below:

UTRAN cell 5 as in TS 36.508

Related ICS/IXIT Statement(s)

- UE supports initiating a session (Yes/No)
- UE supports IMS emergency services (Yes/No)

Test procedure applicable for a UE with UTRA support (TS 34.229-2 [5] A.18/2)

1. IMS emergency call is initiated on the UE.

2-20. UE executes the procedures described in TS 36.508 [94] table [FFS] steps [FFS] for GMM Emergency registration, GPRS emergency bearer context activation, IMS emergency speech call establishment with PSAP.

21. Emergency call is released.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			User initiates an emergency call	
2-6			Steps defined in annex C.22	Generic test procedure for setting up emergency speech call.. Referred from 36.508 [94] table [FFS] for a UE with UTRA support.
7	→		BYE	The UE releases the emergency call
8	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

INVITE (step 1 in procedure in Annex C.22)

Use the default message 'INVITE for MO call setup' in annex A.2.1. with the following conditions:

- A6 'INVITE for creating an emergency session in case of no registration' shall apply;

19.4.3.5 Test requirements

In steps 2-6, UE establishes an emergency call

19.4.4 Emergency call without emergency registration / GPRS / UE contains an ISIM or USIM / UE is in state GMM-REGISTERED.LIMITED-SERVICE

19.4.4.1 Definition and applicability

Test to verify that the UE with ISIM or USIM and in state GMM-REGISTERED.LIMITED-SERVICE, establishes an emergency call if emergency call is initiated, The process consists of setting the emergency call. without any IMS (non emergency or emergency) registration.

19.4.4.2 Conformance requirement

[TS 24.229 clause B.2.2.6]:

Emergency bearers are defined for use in emergency calls in GPRS and core network support of these bearers is indicated to the UE in NAS signalling. Where the UE recognises that a call request is an emergency call and the core network supports emergency bearers, the UE shall use these bearers for both signalling and media on emergency calls made using the IM CN subsystem.

Some jurisdictions allow emergency calls to be made when the UE does not contain an ISIM or USIM, or where the credentials are not accepted. Additionally where the UE is in state GMM-REGISTERED.LIMITED-SERVICE and GMM-REGISTERED.PLMN-SEARCH, a normal ATTACH has been attempted and it can also be assumed that a registration in the IM CN subsystem will also fail. In such cases, the procedures for emergency calls without registration apply, as defined in subclause 5.1.6.8.2.

When activating a PDP context to perform emergency registration, the UE shall request a PDP context for emergency bearer services as defined in 3GPP TS 24.008 [8]. The procedures for PDP context activation and P-CSCF discovery, as described in subclause B.2.2.1 of this specification apply accordingly.

In order to find out whether the UE is attached to the home PLMN or to the visited PLMN, the UE shall compare the MCC and MNC values derived from its IMSI with the MCC and MNC of the PLMN the UE is attached to. If the MCC and MNC of the PLMN the UE is attached to do not match with the MCC and MNC derived from the IMSI, then for the purpose of emergency calls in the IM CN subsystem the UE shall consider to be attached to a VPLMN.

NOTE: In this respect an equivalent HPLMN, as defined in 3GPP TS 23.122 [4C] will be considered as a visited network.

[TS 24.229 clause 5.1.6.8.2]:

When establishing an emergency session for an unregistered user, the UE is allowed to receive responses to emergency requests and requests inside an established emergency session on the unprotected ports. The UE shall reject or silently discard all other messages not arriving on a protected port. Additionally, the UE shall transmit signalling packets pertaining to the emergency session from the same IP address and unprotected port on which it expects to receive signalling packets containing the responses to emergency requests and the requests inside the established emergency session.

Prior to establishing an emergency session for an unregistered user, the UE shall acquire a local IP address, discover a P-CSCF, and establish an IP-CAN bearer that can be used for SIP signalling. The UE shall send only the initial INVITE requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any

specific port information during the P-CSCF discovery procedure, the UE shall send the initial INVITE request to the SIP default port values as specified in RFC 3261 [26].

The UE shall apply the procedures as specified in subclause 5.1.2A.1 and subclause 5.1.3 with the following additions:

1) the UE shall set the From header field of the INVITE request to "Anonymous" as specified in RFC 3261 [26];

2) the UE shall include a Request-URI in the initial INVITE request that contains an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69]. An additional sub-service type can be added if information on the type of emergency service is known;

NOTE 1: Other specifications make provision for emergency service identifiers that are not specifically the emergency service URN, to be recognised in the UE. Emergency service identifiers which the UE does not detect will be treated as a normal call by the UE.

3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;

4) if available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall include in the P-Access-Network-Info header field in any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request. The UE shall populate the P-Access-Network-Info header field with the current point of attachment to the IP-CAN as specified for the access network technology (see subclause 7.2A.4). The P-Access-Network-Info header field contains the location identifier such as the cell id, the line id or the identity of the I-WLAN access node, which is relevant for routeing the emergency call;

5) if defined by the access technology specific annex, the UE shall populate the P-Preferred-Identity header field in the INVITE request with an equipment identifier as a SIP URI. The special details of the equipment identifier to use depends on the IP-CAN;

6) a Contact header field set to include SIP URI that contains in the hostport parameter the IP address of the UE and an unprotected port where the UE will receive incoming requests belonging to this dialog. The UE shall also include a "sip.instance" media feature tag containing Instance ID as described in RFC 5626 [92]. The UE shall not include either the public or temporary GRUU in the Contact header field;

7) a Via header field set to include the IP address of the UE in the sent-by field and for the UDP the unprotected server port value where the UE will receive response to the emergency request, while for the TCP, the response is received on the TCP connection on which the emergency request was sent. For the UDP, the UE shall also include "rport" header field parameter with no value in the top Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with, and during the lifetime of, the emergency session, as described in draft-ietf-sipcore-keep [143];

NOTE 2: The UE inserts the same IP address and port number into the Contact header field and the Via header field, and sends all IP packets to the P-CSCF from this IP address and port number.

8) if the UE has its location information available, the UE shall include the location information in the INVITE request in the following way:

   - if the UE is aware of the URI that points to where the UE's location is stored, include the URI in the Geolocation header field, in accordance with RFC 6442 [98]; or

   - if the geographical location information of the UE is available to the UE, include its geographical location information as PIDF location object in accordance with RFC 4119 [90] and include the location object in a message body with the content type application/pidf+xml in accordance with RFC 6442 [98]. The Geolocation header field is set to a Content ID, in accordance with RFC 6442 [98]; and

9) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in RFC 6442 [98] in the INVITE request.

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is inapplicable in this area.

NOTE 4: During the dialog, the points of attachment to the IP-CAN of the UE can change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header field in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header field value for all new dialogs. The UE shall build a Route header field value containing only the P-CSCF URI (containing the unprotected port number and the IP address or the FQDN learnt through the P-CSCF discovery procedures).

When a SIP transaction times out, i.e. timer B, timer F or timer H expires at the UE, the UE may behave as if timer F expired, as described in subclause 5.1.1.4.

NOTE 5: It is an implementation option whether these actions are also triggered by other means.

NOTE 6: A number of header fields can reveal information about the identity of the user. Where privacy is required, implementers should also give consideration to other header fields that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of header fields.

NOTE 7: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

If the response for the initial INVITE request indicates that the UE is behind NAT, and the INVITE request was sent over TCP connection, the UE shall keep the TCP connection during the entire duration of the emergency session. In this case the UE will receive all responses to the emergency requests and the requests inside the established emergency session over this TCP connection.

If the Via header field of any provisional response, or of the final 200 (OK) response, for the initial INVITE request contains a "keep" header field parameter with a value, unless the UE detects that it is not behind a NAT, the UE shall start to send keep-alives associated with the session towards the P-CSCF, as described in draft-ietf-sipcore-keep [143].

Reference(s)

3GPP TS 24.229[10], clauses 5.1.6.8.2 and Annex B.2.2.6 (release 9)

19.4.4.3 Test purpose

1) To verify that the UE in state GMM-REGISTERED.LIMITED-SERVICE, not registered for non emergency services , on initiation of an emergency call, performs GMM emergency attach to acquire a local IP address, discover a P-CSCF, and establish an IP-CAN bearer that can be used for SIP signalling and then composed INVITE request for the emergency call setup and will correctly complete the emergency session setup using SDP preconditions, according to 3GPP TS 24.229 [10] clauses 5.1.6.8.2 and 6.1.2.

19.4.4.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is in state GMM-REGISTERED.LIMITED-SERVICE; Not registered to IMS services, [FFS: can be achieved by rejecting the Routing Area Update procedure with cause #15, No suitable cells in tracking area; UE is initially registered in cell 5 and made to select cell 7. The Routing area update procedure is rejected with cause #15 in cell 7],

SS is configured with the IMSI within the USIM application, the home domain name, SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS supports GMM emergency attach procedure and PDP context establishment for emergency bearers.

The SS configures two cells as below:

UTRAN cell 5 and 7 as in TS 36.508; Configured cells belong to different LAI

Related ICS/IXIT Statement(s)

- UE supports initiating a session (Yes/No)

- UE supports IMS emergency services (Yes/No)

Test procedure applicable for a UE with UTRA support (TS 34.229-2 [5] A.18/2)

1. IMS emergency call is initiated on the UE.

2-20. UE executes the procedures described in TS 36.508 [94] table [FFS} steps [FFS for GMM Emergency registration, GPRS emergency bearer context activation, IMS emergency speech call establishment with PSAP .

17. Emergency call is released.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			User initiates an emergency call	
2-6			Steps defined in annex C.22	Generic test procedure for setting up emergency speech call. Referred from 36.508 [94] table [FFS] for a UE with UTRA support.
7	→		BYE	The UE releases the emergency call
8	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

INVITE (step 1 in procedure in Annex C.22)

Use the default message 'INVITE for MO call setup' in annex A.2.1. with the following conditions:

- A6 'INVITE for creating an emergency session in case of no registration' shall apply;

19.4.4.5 Test requirements

In steps 2-6, UE establishes an emergency call

19.4.5 Emergency call without emergency registration / UE credentials are not accepted

19.4.5.1 Definition and applicability

Test to verify that when UE is unable to emergency register due to UE credentials not accepted, initiates an emergency call on non protected ports when an emergency call is attempted. The process consists of setting up IMS emergency call after emergency registration failure.

19.4.5.2 Conformance requirement

[TS 24.229 clause 4.2B]:

In case of an emergency session if the UE does not have sufficient credentials to authenticate with the IM CN subsystem and regulations allow, the UE and P-CSCF shall send request and responses other than initial REGISTER requests on non protected ports.

[TS 24.229 clause 4.7]:

The need for support of emergency calls in the IM CN subsystem is determined by national regulatory requirements.

If the UE cannot detect the emergency call attempt, the UE initiates the request as per normal procedures as described in subclause 5.1.2A. Depending on network policies, for a non-roaming UE an emergency call attempt can succeed even if the UE did not detect that an emergency session is being requested, otherwise the network rejects the request indicating to the UE that the attempt was for an emergency service.

The UE procedures for UE detectable emergency calls are defined in subclause 5.1.6.

The P CSCF, S-CSCF, and E-CSCF procedures for emergency service are described in subclause 5.2.10, 5.4.8 and 5.11, respectively.

Access dependent aspects of emergency service (e.g. emergency registration support and location provision) are defined in the access technology specific annexes for each access technology.

There are a number of variants within these procedures and which variant gets used depends on a number of issues. These conditions are defined more specifically in 3GPP TS 23.167 [4B] and, where appropriate, in the access technology specific annex, but are summarised as follows:

a) if the UE knows that it is in its own home network, then an existing registration is permitted to be used for signalling the emergency call, except where item c) applies. The access technology specific annexes define the mechanism by which home network determination is made;

b) if emergency calls are permitted without security credentials (or additionally where the authentication is not possible or has failed), then the emergency call is made directly without use of any security association created by a registration, and therefore without the registration; and

c) where the access technology defines emergency bearers for the support of emergency calls, a new emergency registration is required so that these emergency bearers can be used for both signalling and media, unless an existing emergency registration exists on those emergency bearers.

OK EW

[TS 24.229 clause 5.1.6.1]:

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 [1A] and 3GPP TS 23.167 [4B] to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

The UE shall determine, whether it is currently attached to its home operator's network (e.g. HPLMN) or to a different network than its home operator's network (e.g. VPLMN) by applying access technology specific procedures described in the access technology specific annexes.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is currently registered and the IP-CAN does not define emergency bearers, or the IP-CAN does define emergency bearers but the core network has not indicated that it supports emergency bearers, the UE shall attempt an emergency call as described in subclause 5.1.6.8.4.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is currently registered and the IP-CAN defines emergency bearers and the core network has indicated that it supports emergency bearers, the UE shall:

1) perform an initial emergency registration as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is not currently registered, the UE shall:

1) perform an initial emergency registration, as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE is attached to a different network than its home operator's network (e.g. VPLMN), the UE shall:

1) perform an initial emergency registration, as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE has no credentials the UE can make an emergency call without being registered. The UE shall attempt an emergency call as described in subclause 5.1.6.8.2.

The IP-CAN can, dependant on the IP-CAN capabilities, provide local emergency numbers to the UE which has that capability, in order for the UE to recognize these numbers as emergency call.

A CS and IM CN subsystem capable UE shall follow the conventions and rules specified in 3GPP TS 22.101 [1A] and 3GPP TS 23.167 [4B] to select the domain for the emergency call attempt. If the CS domain is selected, the UE shall attempt an emergency call setup using appropriate access technology specific procedures.

The UE shall determine, whether it is currently attached to its home operator's network (e.g. HPLMN) or to a different network than its home operator's network (e.g. VPLMN) by applying access technology specific procedures described in the access technology specific annexes.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is currently registered and the IP-CAN does not define emergency bearers, the UE shall attempt an emergency call as described in subclause 5.1.6.8.4.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is currently registered and the IP-CAN defines emergency bearers and the core network has indicated that it supports emergency bearers, the UE shall:

1) perform an initial emergency registration as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE is currently attached to its home operator's network (e.g. HPLMN) and the UE is not currently registered, the UE shall:

1) perform an initial emergency registration, as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE is attached to a different network than its home operator's network (e.g. VPLMN), the UE shall:

1) perform an initial emergency registration, as described in subclause 5.1.6.2; and

2) attempt an emergency call as described in subclause 5.1.6.8.3.

If the IM CN subsystem is selected and the UE has no credentials the UE can make an emergency call without being registered. The UE shall attempt an emergency call as described in subclause 5.1.6.8.2.

The IP-CAN can, dependent on the IP-CAN capabilities, provide local emergency numbers (including information about emergency service categories) to the UE which has that capability, in order for the UE to recognize these numbers as emergency call.

[TS 24.229 clause 5.1.6.8.2]:

When establishing an emergency session for an unregistered user, the UE is allowed to receive responses to emergency requests and requests inside an established emergency session on the unprotected ports. The UE shall reject or silently discard all other messages not arriving on a protected port. Additionally, the UE shall transmit signalling packets pertaining to the emergency session from the same IP address and unprotected port on which it expects to receive signalling packets containing the responses to emergency requests and the requests inside the established emergency session.

Prior to establishing an emergency session for an unregistered user, the UE shall acquire a local IP address, discover a P-CSCF, and establish an IP-CAN bearer that can be used for SIP signalling. The UE shall send only the initial INVITE requests to the port advertised to the UE during the P-CSCF discovery procedure. If the UE does not receive any specific port information during the P-CSCF discovery procedure, the UE shall send the initial INVITE request to the SIP default port values as specified in RFC 3261 [26].

The UE shall apply the procedures as specified in subclause 5.1.2A.1 and subclause 5.1.3 with the following additions:

1) the UE shall set the From header field of the INVITE request to "Anonymous" as specified in RFC 3261 [26];

2) the UE shall include a Request-URI in the initial INVITE request that contains an emergency service URN, i.e. a service URN with a top-level service type of "sos" as specified in RFC 5031 [69]. An additional sub-service type can be added if information on the type of emergency service is known;

NOTE 1: Other specifications make provision for emergency service identifiers that are not specifically the emergency service URN, to be recognised in the UE. Emergency service identifiers which the UE does not detect will be treated as a normal call by the UE.

3) the UE shall insert in the INVITE request, a To header field with the same emergency service URN as in the Request-URI;

4) if available to the UE (as defined in the access technology specific annexes for each access technology), the UE shall include in the P-Access-Network-Info header field in any request for a dialog, any subsequent request (except ACK requests and CANCEL requests) or response (except CANCEL responses) within a dialog or any request. The UE shall populate the P-Access-Network-Info header field with the current point of attachment to the IP-CAN as specified for the access network technology (see subclause 7.2A.4). The P-Access-Network-Info header field contains the location identifier such as the cell id, the line id or the identity of the I-WLAN access node, which is relevant for routeing the emergency call;

5) if defined by the access technology specific annex, the UE shall populate the P-Preferred-Identity header field in the INVITE request with an equipment identifier as a SIP URI. The special details of the equipment identifier to use depends on the IP-CAN;

6) a Contact header field set to include SIP URI that contains in the hostport parameter the IP address of the UE and an unprotected port where the UE will receive incoming requests belonging to this dialog. The UE shall also include a "sip.instance" media feature tag containing Instance ID as described in RFC 5626 [92]. The UE shall not include either the public or temporary GRUU in the Contact header field;

7) a Via header field set to include the IP address of the UE in the sent-by field and for the UDP the unprotected server port value where the UE will receive response to the emergency request, while for the TCP, the response is received on the TCP connection on which the emergency request was sent. For the UDP, the UE shall also include "rport" header field parameter with no value in the top Via header field. Unless the UE has been configured to not send keep-alives, and unless the UE is directly connected to an IP-CAN for which usage of NAT is not defined, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate support of sending keep-alives associated with, and during the lifetime of, the emergency session, as described in draft-ietf-sipcore-keep [143];

NOTE 2: The UE inserts the same IP address and port number into the Contact header field and the Via header field, and sends all IP packets to the P-CSCF from this IP address and port number.

8) if the UE has its location information available, the UE shall include the location information in the INVITE request in the following way:

   - if the UE is aware of the URI that points to where the UE's location is stored, include the URI in the Geolocation header field, in accordance withRFC 6442 [98]; or

   - if the geographical location information of the UE is available to the UE, include its geographical location information as PIDF location object in accordance with RFC 4119 [90] and include the location object in a message body with the content type application/pidf+xml in accordance with RFC 6442 [98]. The Geolocation header field is set to a Content ID, in accordance with RFC 6442 [98]; and

9) if the UE has no geographical location information available, the UE shall not include any geographical location information as specified in RFC 6442 [98] in the INVITE request.

NOTE 3: It is suggested that UE's only use the option of providing a URI when the domain part belongs to the current P-CSCF or S-CSCF provider. This is an issue on which the network operator needs to provide guidance to the end user. A URI that is only resolvable to the UE which is making the emergency call is inapplicable in this area.

NOTE 4: During the dialog, the points of attachment to the IP-CAN of the UE can change (e.g. UE connects to different cells). The UE will populate the P-Access-Network-Info header field in any request or response within a dialog with the current point of attachment to the IP-CAN (e.g. the current cell information).

The UE shall build a proper preloaded Route header field value for all new dialogs. The UE shall build a Route header field value containing only the P-CSCF URI (containing the unprotected port number and the IP address or the FQDN learnt through the P-CSCF discovery procedures).

When a SIP transaction times out, i.e. timer B, timer F or timer H expires at the UE, the UE may behave as if timer F expired, as described in subclause 5.1.1.4.

NOTE 5: It is an implementation option whether these actions are also triggered by other means.

NOTE 6: A number of header fields can reveal information about the identity of the user. Where privacy is required, implementers should also give consideration to other header fields that can reveal identity information. RFC 3323 [33] subclause 4.1 gives considerations relating to a number of header fields.

NOTE 7: RFC 3261 [26] provides for the use of the Priority header field with a suggested value of "emergency". It is not precluded that emergency sessions contain this value, but such usage will have no impact on the processing within the IM CN subsystem.

If the response for the initial INVITE request indicates that the UE is behind NAT, and the INVITE request was sent over TCP connection, the UE shall keep the TCP connection during the entire duration of the emergency session. In this case the UE will receive all responses to the emergency requests and the requests inside the established emergency session over this TCP connection.

If the Via header field of any provisional response, or of the final 200 (OK) response, for the initial INVITE request contains a "keep" header field parameter with a value, unless the UE detects that it is not behind a NAT, the UE shall start to send keep-alives associated with the session towards the P-CSCF, as described in draft-ietf-sipcore-keep [143].

[TS 24.229 clause 5.1.1.5.3]:

If, in a 401 (Unauthorized) response, either the MAC or SQN is incorrect the UE shall respond with a further REGISTER indicating to the S-CSCF that the challenge has been deemed invalid as follows:

- in the case where the UE deems the MAC parameter to be invalid the subsequent REGISTER request shall contain no "auts" Authorization header field parameter and an empty "response" Authorization header field parameter, i.e. no authentication challenge response;

- in the case where the UE deems the SQN to be out of range, the subsequent REGISTER request shall contain the "auts" Authorization header field parameter (see 3GPP TS 33.102 [18]).

NOTE 8: In the case of the SQN being out of range, a "response" Authorization header field parameter can be included by the UE, based on the procedures described in RFC 3310 [49].

Whenever the UE detects any of the above cases, the UE shall:

- send the REGISTER request using an existing set of security associations, if available (see 3GPP TS 33.203 [19]);

- populate a new Security-Client header field within the REGISTER request and associated contact address, set to specify the security mechanisms it supports, the IPsec layer algorithms for integrity and confidentiality protection it supports and the parameters needed for the new security association setup; and

- not create a temporary set of security associations.

On receiving a 420 (Bad Extension) in which the Unsupported header field contains the value "sec-agree" and if the UE supports GPRS-IMS-Bundled authentication, the UE shall initiate a new authentication attempt with the GPRS-IMS-Bundled authentication procedures as specified in subclause 5.1.1.2.6.

[TS 24.229 clause 5.1.1.5.12]:

A UE shall only respond to two consecutive invalid challenges and shall not automatically attempt authentication after two consecutive failed attempts to authenticate. The UE may attempt to register with the network again after an implementation specific time.

Reference(s)

3GPP TS 24.229[10], clauses 4.2A, 4.7, 5.1.6.1, 5.1.6.8.2, 5.1.1.5.3 and 5.1.1.5.12.

19.4.5.3 Test purpose

1) To verify that when not registered to IMS services the UE is able to request activation of EPS emergency bearer contexts, according to 3GPP TS 24.229 [10] annex L.2.2.6; and

2) To verify that the UE sends a correctly composed initial REGISTER request for emergency services to S-CSCF via the discovered P-CSCF, according to 3GPP TS 24.229 [10] clause 5.1.6.1; and

3) To verify that the on emergency registration failure, UE continues with the emergency call on non protected ports.

4) To verify that the UI sends a correctly composed INVITE request for the emergency call setup and will correctly complete the emergency session setup using SDP preconditions, according to 3GPP TS 24.229 [10] clauses 5.1.6.8.3 and 6.1.2.

19.4.5.4 Method of test

Initial conditions

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is not registered to IMS services but it is attached to the HPLMN E-UTRA service as provided by SS. In the attach SS has indicated that the cell supports E-UTRA emergency bearers.

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols.

Test environment shall be set up to send in response to Emergency REGISTER message a 401 Unauthorized such that UE will not be able to establish temporary set of security associations.

Related ICS/IXIT Statement(s)

- UE supports IMS emergency services (Yes/No)
- UE supports IPSec ESP confidentiality protection (Yes/No)
- IMS security (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) IMS emergency call is initiated on the UE.

2-13) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 12 (parallel behaviour steps 1) for EPS emergency bearer context activation, IMS emergency speech call establishment with PSAP 14) UE sends initial REGISTER message.

15) The SS responds to the initial REGISTER request with a valid 401 Unauthorized response.

16) The SS waits for the UE to set up a temporary set of security associations and to send another REGISTER request, over those security associations.

18) The SS responds REGISTER message with 403 Forbidden and ignores any further REGISTER message reception.

19-21) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 13 to 15 (parallel behaviour steps 6-10) IMS emergency speech call establishment with PSAP.

22) The Call is released on the UE. SS waits the UE to send a BYE request.

23) The SS responds to the BYE request with valid 200 OK response. Expected sequence.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1			User initiates an emergency call	
2-13			EPS emergency bearer context activation by the UE.	Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support
14	→		REGISTER	The UE sends initial IMS emergency registration
15	←		401 Unauthorized	
16	→		REGISTER	The UE completes the security negotiation procedures, sets up a temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials.
				Note: From this point onward the SS shall ignore any Registration message sent by the UE.
17	←		403 Forbidden	The SS sends this message to get the UE in a stable state.
18-22			Steps defined in annex C.22	IMS emergency call setup with PSAP. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
23	→		BYE	The UE releases the call with BYE (message exchanged on non protected port)
24	←		200 OK	The SS sends 200 OK for BYE (message exchanged on non protected port)

Specific Message Contents

INVITE (. step 1 of Annex C.22)

Use the default message 'INVITE for MO call setup' in annex A.2.1. with the following conditions:

- A6 'INVITE for creating an emergency session in case of no registration' shall apply;

180 Ringing for INVITE (step 3 of Annex C.22)

Use the default message '180 Ringing for INVITE' in annex A.2.6. The condition A4 '180 sent by the SS when setting up an emergency call' shall apply.

200 OK for INVITE (Step 20 i.e. step 4 of Annex C.22)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1. The condition A6 'Response sent by SS for INVITE for emergency call' shall apply.

REGISTER (Step 14)

Use the default message 'REGISTER' in annex A.1.1 with condition A1.

401 UNAUTHORIZED (Steps 15)

Use the default message '401 Unauthorized for REGISTER' in annex A.1.2

REGISTER (Steps 16)

Use the default message 'REGISTER' in annex A.1.1 with condition A2.

403 FORBIDDEN (Step 17)

Use the default message '403 FORBIDDEN' in annex A.3.2

BYE (Step 23)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE (Step 24)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

19.4.5.5 Test requirements

In step 2-13 UE performs EMM emergency registration and emergency EPS bearer context.

In steps 18-22, UE establishes an emergency call.

19.5 Emergency registration

19.5.1 New initial emergency registration / UE obtains from the serving IP-CAN an IP address different than the IP address used for the emergency registration

19.5.1.1 Definition and applicability

Test to verify that the UE performed emergency registration which has not yet expired, triggers new initial emergency registration , when UE obtains a different IP address than used for current emergency registration. The process consists of sending a new REGISTER request over the existing security associations and EPS emergency bearers, receiving 401 response, sending another REGISTER request to complete the reauthentication and receiving the 200 OK for renewed registration. The test case is applicable for IMS security.

19.5.1.2 Conformance requirement

[TS 24.229 clause 5.1.6.2A]:

The UE shall perform a new initial emergency registration, as specified in subclause 5.1.6.2, if the UE determines that:

- it has previously performed an emergency registration which has not yet expired; and
- it has obtained an IP address from the serving IP-CAN, as specified in subclause 9.2.1, different than the IP address used for the emergency registration.

[TS 24.229 clause 5.1.1.4.1]:

When sending a protected REGISTER request, the UE shall use a security association or TLS session associated with the contact address used to send the request, see 3GPP TS 33.203 [19], established as a result of an earlier initial registration.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) that contain(s) in the hostport parameter the IP address or FQDN of the UE, and containing the instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations. If the UE support multiple registrations, it shall include "reg-id" header field as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication it intends to use, and IARI values (coded as

specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62];

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field. For the TCP, the response is received on the TCP connection on which the request was sent. If the UE previously has previously negotiated sending of keep-alives associated with the registration, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate continuous support to send keep-alives, as described in draft-ietf-sipcore-keep [143];

e) a registration expiration interval value, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 1: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and if GRUU is supported, the option-tag "gruu";

h) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174].

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) bind the new expiration time of the registration for this public user identity found in the To header field value to the contact address used in this registration;

b) store the list of service route values contained in the Service-Route header field and bind the list to the contact address used in registration, in order to build a proper preloaded Route header field value for new dialogs and standalone transactions when using the respective contact address;

NOTE 3: If the list of Service-Route headers saved from a previous registration and bound to this contact address and the associated set of security associations or TLS session already exist, then the received list of Service-Route headers replaces the old list.

NOTE 4: The UE can utilize additional URIs contained in the P-Associated-URI header field, e.g. for application purposes.

c) find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, and the UE supports GRUU (see table A.4, item A.4/53), then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered;

d) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174]; and

NOTE 5: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

e) if the Via header field contains a "keep" header field parameter with a value, continue to send keep-alives as described in draft-ietf-sipcore-keep [143], towards the P-CSCF.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

[TS 24.229 clause 5.1.1.4.2]:

On sending a REGISTER request, as defined in subclause 5.1.1.4.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field, with:

- the "username" header field parameter set to the value of the private user identity;
- the "realm" header field parameter directive, set to the value as received in the "realm" WWW-Authenticate header field parameter;
- the "uri" header field parameter, set to the SIP URI of the domain name of the home network;
- the "nonce" header field parameter, set to last received nonce value; and
- the "response" header field parameter, set to the last calculated response value;

NOTE 1: If the UE specifies its FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

NOTE 3: If the UE is setting up an additional registration using procedures specified in RFC 5626 [92] and the UE accesses the network through 3GPP or 3GPP2 systems without any NAT, the flow is considered to be "logical flow".

b) additionally for the Contact header field, include the protected server port value in the hostport parameter;

c) additionally for the Via header field, for UDP, if the REGISTER request is protected by a security association, include the protected server port value in the sent-by field;

d) a Security-Client header field, set to specify the signalling plane security mechanism it supports, the IPsec layer algorithms for security and confidentiality protection it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]; and

e) a Security-Verify header field that contains the content of the Security-Server header field received in the 401 (Unauthorized) response of the last successful authentication.

On receiving the 200 (OK) response to the REGISTER request, the UE shall additionally:

a) set the security association lifetime associated with this contact address and the associated set of security associations to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds.

[TS 24.229 clause 5.1.1.5.1]:

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

1) extract the RAND and AUTN parameters;

2) check the validity of a received authentication challenge, as described in 3GPP TS 33.203 [19] i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

3) check the existence of the Security-Server header field as described in RFC 3329 [48]. If the Security-Server header field is not present or it does not contain the parameters required for the setup of the set of security associations (see annex H of 3GPP TS 33.203 [19]), the UE shall abandon the authentication procedure and send a new REGISTER request with a new Call-ID.

In the case that the 401 (Unauthorized) response to the REGISTER request is deemed to be valid the UE shall:

1) calculate the RES parameter and derive the keys CK and IK from RAND as described in 3GPP TS 33.203 [19];

2) set up a temporary set of security associations for this registration based on the static list and parameters the UE received in the 401 (Unauthorized) response and its capabilities sent in the Security-Client header field in the REGISTER request. The UE sets up the temporary set of security associations using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE and using IK and CK (only if

encryption enabled) as the shared key. The UE shall use the parameters received in the Security-Server header field to setup the temporary set of security associations. The UE shall set a temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer;

3) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174].

NOTE 1: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

4) send another REGISTER request towards the protected server port indicated in the response using the temporary set of security associations to protect the message. The header fields are populated as defined for the initial REGISTER request that was challenged with the received 401 (Unauthorized) response, with the addition that the UE shall include an Authorization header field containing:

- the "realm" header field parameter set to the value as received in the "realm" WWW-Authenticate header field parameter;
- the "username" header field parameter, set to the value of the private user identity;
- the "response" header field parameter that contains the RES parameter, as described in RFC 3310 [49];
- the "uri" header field parameter, set to the SIP URI of the domain name of the home network;
- the "algorithm" header field parameter, set to the value received in the 401 (Unauthorized) response; and
- the "nonce" header field parameter, set to the value received in the 401 (Unauthorized) response.

The UE shall also insert the Security-Client header field that is identical to the Security-Client header field that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header field into the request, by mirroring in it the content of the Security-Server header field received in the 401 (Unauthorized) response. The UE shall set the Call-ID of the security association protected REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

On receiving the 200 (OK) response for the security association protected REGISTER request registering a public user identity with the associated contact address, the UE shall:

- change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and
- if this is the only set of security associations available toward the P-CSCF, use the newly established set of security associations for further messages sent towards the P-CSCF. If there are additional sets of security associations (e.g. due to registration of multiple contact addresses), the UE can either use them or use the newly established set of security associations for further messages sent towards the P-CSCF as appropriate.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.6.2A, 5.1.1.4.2, 5.1.1.5.1 and 5.1.6.4 (release 9)

19.5.1.3 Test purpose

1) To verify that when UE obtains an IP address different than the IP address used for current emergency registration, not yet expired, the UE shall perform new initial emergency registration, as defined within 3GPP TS 24.229 [10] clauses 5.1.6.2A.

19.5.1.4 Method of test

Initial conditions

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE contains either ISIM and USIM applications or only USIM application on UICC. In the E-UTRA attach SS has indicated to the UE that the cell supports E-UTRA emergency bearers. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step. UE has registered to IMS emergency services, by executing the generic test procedure in Annex C.20 up to the last step. Thereafter the UE has initiated an emergency call by executing the generic test procedure in Annex C.22 up to the last step. The emergency call is released;

Trigger an IP address re=allocation; This is done by executing a network initiated detach procedure with detach type indicates "re-attach required". The UE then triggers an Attach procedure; The SS indicates support of emergency bearers and allocates an IP address different than the attach procedure in preamble.

Related ICS/IXIT Statement(s)

- UE supports IMS emergency services (Yes/No)
- UE supports IPSec ESP confidentiality protection (Yes/No)
- IMS security (Yes/No)

Test procedure

applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-15) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 15 for EPS emergency bearer context activation, IMS emergency registration and subsequent IMS emergency speech call establishment with PSAP

16) Call is released on the UE. SS waits the UE to send a BYE request.

17) SS responds to the BYE request with valid 200 OK response. Expected sequence.

Step	Direction		Message	Comment
	UE	SS		
1			User initiates an emergency call	
2-10			Steps defined in annex C.20 followed by the steps defined in annex C.22	IMS emergency registration by the UE followed by IMS emergency call setup with PSAP. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
11	→		BYE	The UE releases the call with BYE
12	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

INVITE (. step 1 of Annex C.22)

Use the default message 'INVITE for MO call setup' in annex A.2.1. with the following conditions:

- A7 'INVITE for creating an emergency session within an emergency registration' shall apply; and
- A8 'UE uses Geolocation header to provide its geographical location for emergency session setup, has obtained its location and is setting up an emergency session ' shall apply if the UE uses Geolocation header to provide its geographical location for emergency session setup.

180 Ringing for INVITE (step 3 of Annex C.22)

Use the default message '180 Ringing for INVITE' in annex A.2.6. The condition A4 '180 sent by the SS when setting up an emergency call' shall apply.

200 OK for INVITE (step 4 of Annex C.22)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1. The condition A6 'Response sent by SS for INVITE for emergency call' shall apply

BYE (Step 11)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE (Step 12)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

19.5.1.5 Test requirements

In step 2-10 UE performs emergency EPS bearer context establishment and establishes an emergency call.

19.5.2 to 19.5.5

19.5.6 User-initiated emergency reregistration / UE has emergency related ongoing dialog

19.5.6.1 Definition and applicability

Test to verify that the UE can correctly renew its emergency registration while an emergency call is going on and half of the registration time has expired. The process consists of sending a new REGISTER request over the existing security associations and EPS emergency bearers, receiving 401 response, sending another REGISTER request to complete the reauthentication and receiving the 200 OK for renewed registration. The test case is applicable for IMS security.

19.5.6.2 Conformance requirement

[TS 24.229 clause 5.1.6.4]:

The UE shall perform user-initiated emergency reregistration as specified in subclause 5.1.1.4 if half of the time for the emergency registration has expired and:

- the UE has emergency related ongoing dialog; or
- standalone transactions exist; or
- the user initiates an emergency call.

[TS 24.229 clause 5.1.1.4.1]:

When sending a protected REGISTER request, the UE shall use a security association or TLS session associated with the contact address used to send the request, see 3GPP TS 33.203 [19], established as a result of an earlier initial registration.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) that contain(s) in the hostport parameter the IP address or FQDN of the UE, and containing the instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations. If the UE support multiple registrations, it shall include "reg-id" header field as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62];

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field. For the TCP, the response is received on the TCP connection on which the request was sent. If the UE previously has previously negotiated sending of keep-alives associated with the registration, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate continuous support to send keep-alives, as described in draft-ietf-sipcore-keep [143];

e) a registration expiration interval value, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 1: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and if GRUU is supported, the option-tag "gruu";

h) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174].

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) bind the new expiration time of the registration for this public user identity found in the To header field value to the contact address used in this registration;

b) store the list of service route values contained in the Service-Route header field and bind the list to the contact address used in registration, in order to build a proper preloaded Route header field value for new dialogs and standalone transactions when using the respective contact address;

NOTE 3: If the list of Service-Route headers saved from a previous registration and bound to this contact address and the associated set of security associations or TLS session already exist, then the received list of Service-Route headers replaces the old list.

NOTE 4: The UE can utilize additional URIs contained in the P-Associated-URI header field, e.g. for application purposes.

c) find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, and the UE supports GRUU (see table A.4, item A.4/53), then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered;

d) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174]; and

NOTE 5: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

e) if the Via header field contains a "keep" header field parameter with a value, continue to send keep-alives as described in draft-ietf-sipcore-keep [143], towards the P-CSCF.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

[TS 24.229 clause 5.1.1.4.2]:

On sending a REGISTER request, as defined in subclause 5.1.1.4.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field, with:

- the "username" header field parameter set to the value of the private user identity;
- the "realm" header field parameter directive, set to the value as received in the "realm" WWW-Authenticate header field parameter;
- the "uri" header field parameter, set to the SIP URI of the domain name of the home network;
- the "nonce" header field parameter, set to last received nonce value; and
- the "response" header field parameter, set to the last calculated response value;

NOTE 1: If the UE specifies its FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

NOTE 3: If the UE is setting up an additional registration using procedures specified in RFC 5626 [92] and the UE accesses the network through 3GPP or 3GPP2 systems without any NAT, the flow is considered to be "logical flow".

b) additionally for the Contact header field, include the protected server port value in the hostport parameter;

c) additionally for the Via header field, for UDP, if the REGISTER request is protected by a security association, include the protected server port value in the sent-by field;

d) a Security-Client header field, set to specify the signalling plane security mechanism it supports, the IPsec layer algorithms for security and confidentiality protection it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]; and

e) a Security-Verify header field that contains the content of the Security-Server header field received in the 401 (Unauthorized) response of the last successful authentication.

On receiving the 200 (OK) response to the REGISTER request, the UE shall additionally:

a) set the security association lifetime associated with this contact address and the associated set of security associations to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds.

[TS 24.229 clause 5.1.1.5.1]:

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

1) extract the RAND and AUTN parameters;

2) check the validity of a received authentication challenge, as described in 3GPP TS 33.203 [19] i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

3) check the existence of the Security-Server header field as described in RFC 3329 [48]. If the Security-Server header field is not present or it does not contain the parameters required for the setup of the set of security associations (see annex H of 3GPP TS 33.203 [19]), the UE shall abandon the authentication procedure and send a new REGISTER request with a new Call-ID.

In the case that the 401 (Unauthorized) response to the REGISTER request is deemed to be valid the UE shall:

1) calculate the RES parameter and derive the keys CK and IK from RAND as described in 3GPP TS 33.203 [19];

2) set up a temporary set of security associations for this registration based on the static list and parameters the UE received in the 401 (Unauthorized) response and its capabilities sent in the Security-Client header field in the REGISTER request. The UE sets up the temporary set of security associations using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE and using IK and CK (only if encryption enabled) as the shared key. The UE shall use the parameters received in the Security-Server header field to setup the temporary set of security associations. The UE shall set a temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer;

3) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174].

NOTE 1: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

4) send another REGISTER request towards the protected server port indicated in the response using the temporary set of security associations to protect the message. The header fields are populated as defined for the initial REGISTER request that was challenged with the received 401 (Unauthorized) response, with the addition that the UE shall include an Authorization header field containing:

   - the "realm" header field parameter set to the value as received in the "realm" WWW-Authenticate header field parameter;

   - the "username" header field parameter, set to the value of the private user identity;

   - the "response" header field parameter that contains the RES parameter, as described in RFC 3310 [49];

   - the "uri" header field parameter, set to the SIP URI of the domain name of the home network;

   - the "algorithm" header field parameter, set to the value received in the 401 (Unauthorized) response; and

   - the "nonce" header field parameter, set to the value received in the 401 (Unauthorized) response.

   The UE shall also insert the Security-Client header field that is identical to the Security-Client header field that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header field into the request, by mirroring in it the content of the Security-Server header field received in the 401 (Unauthorized) response. The UE shall set the Call-ID of the security association protected REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

On receiving the 200 (OK) response for the security association protected REGISTER request registering a public user identity with the associated contact address, the UE shall:

- change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and

- if this is the only set of security associations available toward the P-CSCF, use the newly established set of security associations for further messages sent towards the P-CSCF. If there are additional sets of security associations (e.g. due to registration of multiple contact addresses), the UE can either use them or use the newly established set of security associations for further messages sent towards the P-CSCF as appropriate.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.1.4.1, 5.1.1.4.2, 5.1.1.5.1 and 5.1.6.4 (release 9)

19.5.6.3 Test purpose

1) To verify that when half of the time for the emergency registration has expired and the UE has emergency related ongoing dialog, the UE shall perform user-initiated emergency reregistration, as defined within 3GPP TS 24.229 [10] clauses 5.1.6.4, 5.1.1.4.1, 5.1.1.4.2 and 5.1.1.5.1.

19.5.6.4 Method of test

Initial conditions

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE contains either ISIM and USIM applications or only USIM application on UICC. In the E-UTRA attach SS has indicated to the UE that the cell supports E-UTRA emergency bearers. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step. The UE has performed EPS emergency bearer context activation, IMS emergency registration and the subsequent IMS emergency call, s described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 15. When performing the steps of Annex C.20 the SS sets the expiration time to 120 seconds in Step 6. Thereafter the UE has initiated an emergency call by executing the generic test procedure in Annex C.22 up to the last step.

Related ICS/IXIT Statement(s)

- UE supports IMS emergency services (Yes/No)
- UE supports IPSec ESP confidentiality protection (Yes/No)
- IMS security (Yes/No)
- obtaining and using GRUUs in the Session Initiation Protocol (SIP) (Yes/No)

Test procedure

1) When half of the initial emergency registration time has expired and while emergency call is still going on SS receives REGISTER request from the UE.
2) SS responds to the REGISTER request with a valid 401 Unauthorized response, headers populated according to the 401 response common message definition.
3) SS waits for the UE to set up a new set of security associations and send another REGISTER request, over those security associations.
4) The SS responds with 200 OK over the new security association, setting the new expiration time as 1200 seconds

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE re-registers to the emergency services 60 seconds before the expected expiration.
2	←		401 Unauthorized	The SS responds with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network.
3	→		REGISTER	UE completes the security negotiation procedures, sets up a new temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials.
4	←		200 OK	The UE responds with 200 OK.

Specific Message Contents

REGISTER (Step 1)

Use the default message 'REGISTER' in annex A.1.1. with condition A2 "Subsequent REGISTER sent over security associations' and the following exceptions applying:

Header/param	Value/remark
Contact	
addr-spec	SIP URI with IP address or FQDN and protected server port of UE. The SIP URI shall contain the *sos* URI parameter.
Security-Client	
spi-c	new SPI number of the inbound SA at the protected client port
spi-s	new SPI number of the inbound SA at the protected server port
port-c	new protected client port needed for the setup of new pairs of security associations
port-s	Same value as in the previous REGISTER

401 Unauthorized for REGISTER (Step 2)

Use the default message '401 Unauthorized for REGISTER' in annex A.1.2 with the following exceptions:

Header/param	Value/remark
Security-Server	
spi-c	new SPI number of the inbound SA at the protected client port
spi-s	new SPI number of the inbound SA at the protected server port
port-c	new protected client port needed for the setup of new pairs of security associations
port-s	Same value as in the previous Security-Server headers
WWW-Authenticate	
nonce	Base 64 encoding of a new RAND and AUTN

REGISTER (Step 3)

Use the default message 'REGISTER' in annex A.1.1 like in step 1 above. The only difference is that the response value within Authorization header shall have been recalculated based on the nonce received from SS within 401 response.

200 OK for REGISTER (Step 4)

Use the default message '200 OK for REGISTER' in annex A.1.3 with condition A3 'Response for an emergency registration' and the expires parameter of Contact header set to 1200.

19.5.6.5 Test requirements

All the messages specified for this test case shall be sent over the EPS emergency bearers allocated for the initial emergency registration.

19.5.7 User-initiated emergency reregistration / The user initiates an emergency call

19.5.7.1 Definition and applicability

Test to verify that the UE can correctly renew its emergency registration while an emergency call is being initiated and half of the registration time has expired. The re-registration process consists of sending a new REGISTER request over the existing security associations and EPS emergency bearers, receiving 401 response, sending another REGISTER request to complete the reauthentication and receiving the 200 OK for renewed registration. The test case is applicable for IMS security.

19.5.7.2 Conformance requirement

[TS 24.229 clause 5.1.6.4]:

The UE shall perform user-initiated emergency reregistration as specified in subclause 5.1.1.4 if half of the time for the emergency registration has expired and:

- the UE has emergency related ongoing dialog; or
- standalone transactions exist; or
- the user initiates an emergency call.

[TS 24.229 clause 5.1.1.4.1]:

When sending a protected REGISTER request, the UE shall use a security association or TLS session associated with the contact address used to send the request, see 3GPP TS 33.203 [19], established as a result of an earlier initial registration.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) that contain(s) in the hostport parameter the IP address or FQDN of the UE, and containing the instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations. If the UE support multiple registrations, it shall include "reg-id" header field as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62];

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field. For the TCP, the response is received on the TCP connection on which the request was sent. If the UE previously has previously negotiated sending of keep-alives associated with the registration, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate continuous support to send keep-alives, as described in draft-ietf-sipcore-keep [143];

e) a registration expiration interval value, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 1: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and if GRUU is supported, the option-tag "gruu";

h) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174].

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) bind the new expiration time of the registration for this public user identity found in the To header field value to the contact address used in this registration;

b) store the list of service route values contained in the Service-Route header field and bind the list to the contact address used in registration, in order to build a proper preloaded Route header field value for new dialogs and standalone transactions when using the respective contact address;

NOTE 3: If the list of Service-Route headers saved from a previous registration and bound to this contact address and the associated set of security associations or TLS session already exist, then the received list of Service-Route headers replaces the old list.

NOTE 4: The UE can utilize additional URIs contained in the P-Associated-URI header field, e.g. for application purposes.

c) find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, and the UE supports GRUU (see table A.4, item A.4/53), then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered;

d) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174]; and

NOTE 5: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

e) if the Via header field contains a "keep" header field parameter with a value, continue to send keep-alives as described in draft-ietf-sipcore-keep [143], towards the P-CSCF.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

[TS 24.229 clause 5.1.1.4.2]:

On sending a REGISTER request, as defined in subclause 5.1.1.4.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field, with:

- the "username" header field parameter set to the value of the private user identity;
- the "realm" header field parameter directive, set to the value as received in the "realm" WWW-Authenticate header field parameter;
- the "uri" header field parameter, set to the SIP URI of the domain name of the home network;
- the "nonce" header field parameter, set to last received nonce value; and
- the "response" header field parameter, set to the last calculated response value;

NOTE 1: If the UE specifies its FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

NOTE 3: If the UE is setting up an additional registration using procedures specified in RFC 5626 [92] and the UE accesses the network through 3GPP or 3GPP2 systems without any NAT, the flow is considered to be "logical flow".

b) additionally for the Contact header field, include the protected server port value in the hostport parameter;

c) additionally for the Via header field, for UDP, if the REGISTER request is protected by a security association, include the protected server port value in the sent-by field;

d) a Security-Client header field, set to specify the signalling plane security mechanism it supports, the IPsec layer algorithms for security and confidentiality protection it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]; and

e) a Security-Verify header field that contains the content of the Security-Server header field received in the 401 (Unauthorized) response of the last successful authentication.

On receiving the 200 (OK) response to the REGISTER request, the UE shall additionally:

a) set the security association lifetime associated with this contact address and the associated set of security associations to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds.

[TS 24.229 clause 5.1.1.5.1]:

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

1) extract the RAND and AUTN parameters;

2) check the validity of a received authentication challenge, as described in 3GPP TS 33.203 [19] i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

3) check the existence of the Security-Server header field as described in RFC 3329 [48]. If the Security-Server header field is not present or it does not contain the parameters required for the setup of the set of security associations (see annex H of 3GPP TS 33.203 [19]), the UE shall abandon the authentication procedure and send a new REGISTER request with a new Call-ID.

In the case that the 401 (Unauthorized) response to the REGISTER request is deemed to be valid the UE shall:

1) calculate the RES parameter and derive the keys CK and IK from RAND as described in 3GPP TS 33.203 [19];

2) set up a temporary set of security associations for this registration based on the static list and parameters the UE received in the 401 (Unauthorized) response and its capabilities sent in the Security-Client header field in the REGISTER request. The UE sets up the temporary set of security associations using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE and using IK and CK (only if encryption enabled) as the shared key. The UE shall use the parameters received in the Security-Server header field to setup the temporary set of security associations. The UE shall set a temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer;

3) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174].

NOTE 1: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

4) send another REGISTER request towards the protected server port indicated in the response using the temporary set of security associations to protect the message. The header fields are populated as defined for the initial REGISTER request that was challenged with the received 401 (Unauthorized) response, with the addition that the UE shall include an Authorization header field containing:

- the "realm" header field parameter set to the value as received in the "realm" WWW-Authenticate header field parameter;

- the "username" header field parameter, set to the value of the private user identity;

- the "response" header field parameter that contains the RES parameter, as described in RFC 3310 [49];
- the "uri" header field parameter, set to the SIP URI of the domain name of the home network;
- the "algorithm" header field parameter, set to the value received in the 401 (Unauthorized) response; and
- the "nonce" header field parameter, set to the value received in the 401 (Unauthorized) response.

The UE shall also insert the Security-Client header field that is identical to the Security-Client header field that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header field into the request, by mirroring in it the content of the Security-Server header field received in the 401 (Unauthorized) response. The UE shall set the Call-ID of the security association protected REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

On receiving the 200 (OK) response for the security association protected REGISTER request registering a public user identity with the associated contact address, the UE shall:

- change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and
- if this is the only set of security associations available toward the P-CSCF, use the newly established set of security associations for further messages sent towards the P-CSCF. If there are additional sets of security associations (e.g. due to registration of multiple contact addresses), the UE can either use them or use the newly established set of security associations for further messages sent towards the P-CSCF as appropriate.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.1.4.1, 5.1.1.4.2, 5.1.1.5.1 and 5.1.6.4 (release 9)

19.5.7.3 Test purpose

1) To verify that when half of the time for the emergency registration has expired and the UE is in the process of initiating an emergency call, the UE shall perform user-initiated emergency reregistration, as defined within 3GPP TS 24.229 [10] clauses 5.1.6.4, 5.1.1.4.1, 5.1.1.4.2 and 5.1.1.5.1.

19.5.7.4 Method of test

Initial conditions

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE contains either ISIM and USIM applications or only USIM application on UICC. In the E-UTRA attach SS has indicated to the UE that the cell supports E-UTRA emergency bearers. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

Related ICS/IXIT Statement(s)

- UE supports IMS emergency services (Yes/No)
- IMS security (Yes/No)

Test procedure

Expected sequence, procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1) Emergency call is initiated on the UE as described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 15 for EPS emergency bearer context activation and subsequent IMS emergency registration. The UE registers to IMS emergency services, by executing the generic test procedure in Annex C.20 up to the last step with the exception that the SS sets the expiration time to 5 seconds in Step 1.

2) After completing the IMS emergency registration UE starts the process of initiating an emergency call, by executing the generic test procedure in steps 1-3 of Annex C.22. However during the steps specified in Annex C.22 the SS shall delay every response sent to the UE by one second, to cause the half of the emergency registration time to expire after step 3 of Annex C.22 (180 response sent by the SS).

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1			Steps defined in annex C.20	EPS emergency bearer context activation and subsequent IMS emergency registration by the UE. SS sets the expiration time of emergency registration to 5 seconds.
2			Steps 1-3 defined in annex C.22 with the exception that SS shall delay every response it sends to UE by 1 second.	IMS emergency call setup with PSAP using preconditions

Expected sequence, parallel behaviour

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE re-registers to the emergency services roughly 2 seconds before the expected expiration.
2	←		401 Unauthorized	The SS responds with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network.
3	→		REGISTER	UE completes the security negotiation procedures, sets up a new temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials.
4	←		200 OK	The UE responds with 200 OK.

Specific Message Contents for parallel behaviour

REGISTER (Step 1)

Use the default message 'REGISTER' in annex A.1.1. with condition A2 "Subsequent REGISTER sent over security associations' and the following exceptions applying:

Header/param	Value/remark
Contact	
addr-spec	SIP URI with IP address or FQDN and protected server port of UE. The SIP URI shall contain the *sos* URI parameter.
Security-Client	
spi-c	new SPI number of the inbound SA at the protected client port
spi-s	new SPI number of the inbound SA at the protected server port
port-c	new protected client port needed for the setup of new pairs of security associations
port-s	Same value as in the previous REGISTER

401 Unauthorized for REGISTER (Step 2)

Use the default message '401 Unauthorized for REGISTER' in annex A.1.2 with the following exceptions:

Header/param	Value/remark
Security-Server	
spi-c	new SPI number of the inbound SA at the protected client port
spi-s	new SPI number of the inbound SA at the protected server port
port-c	new protected client port needed for the setup of new pairs of security associations
port-s	Same value as in the previous Security-Server headers
WWW-Authenticate	
nonce	Base 64 encoding of a new RAND and AUTN

REGISTER (Step 3)

Use the default message 'REGISTER' in annex A.1.1 like in step 1 above. The only difference is that the response value within Authorization header shall have been recalculated based on the nonce received from SS within 401 response.

200 OK for REGISTER (Step 4)

Use the default message '200 OK for REGISTER' in annex A.1.3 with condition A3 'Response for an emergency registration' and the expires parameter of Contact header set to 1200.

19.5.7.5 Test requirements

All the messages specified for this test case shall be sent over the EPS emergency bearers allocated for the initial emergency registration.

19.5.8 User-initiated emergency reregistration / Standalone transactions exist

19.5.8.1 Definition and applicability

Test to verify that the UE can correctly renew its emergency registration while a standalone transaction is pending and half of the registration time has expired. The re-registration process consists of sending a new REGISTER request over the existing security associations and EPS emergency bearers, receiving 401 response, sending another REGISTER request to complete the reauthentication and receiving the 200 OK for renewed registration. The test case is applicable for IMS security.

19.5.8.2 Conformance requirement

[TS 24.229 clause 5.1.6.4]:

The UE shall perform user-initiated emergency reregistration as specified in subclause 5.1.1.4 if half of the time for the emergency registration has expired and:

- the UE has emergency related ongoing dialog; or
- standalone transactions exist; or
- the user initiates an emergency call.

[TS 24.229 clause 5.1.1.4.1]:

When sending a protected REGISTER request, the UE shall use a security association or TLS session associated with the contact address used to send the request, see 3GPP TS 33.203 [19], established as a result of an earlier initial registration.

The UE shall extract or derive a public user identity, the private user identity, and the domain name to be used in the Request-URI in the registration, according to the procedures described in subclause 5.1.1.1A or subclause 5.1.1.1B.

On sending a REGISTER request that does not contain a challenge response, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains the public user identity to be registered;

b) a To header field set to the SIP URI that contains the public user identity to be registered;

c) a Contact header field set to include SIP URI(s) that contain(s) in the hostport parameter the IP address or FQDN of the UE, and containing the instance ID of the UE in the "+sip.instance" header field parameter, if the UE supports GRUU (see table A.4, item A.4/53) or multiple registrations. If the UE support multiple registrations, it shall include "reg-id" header field as described in RFC 5626 [92]. The UE shall include all supported ICSI values (coded as specified in subclause 7.2A.8.2) in a g.3gpp.icsi-ref media feature tag as defined in subclause 7.9.2 and RFC 3840 [62] for the IMS communication it intends to use, and IARI values (coded as specified in subclause 7.2A.9.2), for the IMS applications it intends to use in a g.3gpp.iari-ref media feature tag as defined in subclause 7.9.3 and RFC 3840 [62];

d) a Via header field set to include the IP address or FQDN of the UE in the sent-by field. For the TCP, the response is received on the TCP connection on which the request was sent. If the UE previously has previously negotiated sending of keep-alives associated with the registration, it shall include a "keep" header field parameter with no value in the Via header field, in order to indicate continuous support to send keep-alives, as described in draft-ietf-sipcore-keep [143];

e) a registration expiration interval value, set to 600 000 seconds as the value desired for the duration of the registration;

NOTE 1: The registrar (S-CSCF) might decrease the duration of the registration in accordance with network policy. Registration attempts with a registration period of less than a predefined minimum value defined in the registrar will be rejected with a 423 (Interval Too Brief) response.

f) a Request-URI set to the SIP URI of the domain name of the home network used to address the REGISTER request;

g) the Supported header field containing the option-tag "path", and if GRUU is supported, the option-tag "gruu";

h) if available to the UE (as defined in the access technology specific annexes for each access technology), a P-Access-Network-Info header field set as specified for the access network technology (see subclause 7.2A.4); and

i) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174].

On receiving the 200 (OK) response to the REGISTER request, the UE shall:

a) bind the new expiration time of the registration for this public user identity found in the To header field value to the contact address used in this registration;

b) store the list of service route values contained in the Service-Route header field and bind the list to the contact address used in registration, in order to build a proper preloaded Route header field value for new dialogs and standalone transactions when using the respective contact address;

NOTE 3: If the list of Service-Route headers saved from a previous registration and bound to this contact address and the associated set of security associations or TLS session already exist, then the received list of Service-Route headers replaces the old list.

NOTE 4: The UE can utilize additional URIs contained in the P-Associated-URI header field, e.g. for application purposes.

c) find the Contact header field within the response that matches the one included in the REGISTER request. If this contains a "pub-gruu" header field parameter or a "temp-gruu" header field parameter or both, and the UE supports GRUU (see table A.4, item A.4/53), then store the value of those parameters as the GRUUs for the UE in association with the public user identity and the contact address that was registered;

d) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174]; and

NOTE 5: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

e) if the Via header field contains a "keep" header field parameter with a value, continue to send keep-alives as described in draft-ietf-sipcore-keep [143], towards the P-CSCF.

When a 401 (Unauthorized) response to a REGISTER is received the UE shall behave as described in subclause 5.1.1.5.1.

[TS 24.229 clause 5.1.1.4.2]:

On sending a REGISTER request, as defined in subclause 5.1.1.4.1, the UE shall additionally populate the header fields as follows:

a) an Authorization header field, with:

- the "username" header field parameter set to the value of the private user identity;
- the "realm" header field parameter directive, set to the value as received in the "realm" WWW-Authenticate header field parameter;
- the "uri" header field parameter, set to the SIP URI of the domain name of the home network;
- the "nonce" header field parameter, set to last received nonce value; and
- the "response" header field parameter, set to the last calculated response value;

NOTE 1: If the UE specifies its FQDN in the hostport parameter in the Contact header field and in the sent-by field in the Via header field, then it has to ensure that the given FQDN will resolve (e.g., by reverse DNS lookup) to the IP address that is bound to the security association.

NOTE 2: The UE associates two ports, a protected client port and a protected server port, with each pair of security associations. For details on the selection of the protected port value see 3GPP TS 33.203 [19].

NOTE 3: If the UE is setting up an additional registration using procedures specified in RFC 5626 [92] and the UE accesses the network through 3GPP or 3GPP2 systems without any NAT, the flow is considered to be "logical flow".

b) additionally for the Contact header field, include the protected server port value in the hostport parameter;

c) additionally for the Via header field, for UDP, if the REGISTER request is protected by a security association, include the protected server port value in the sent-by field;

d) a Security-Client header field, set to specify the signalling plane security mechanism it supports, the IPsec layer algorithms for security and confidentiality protection it supports and the new parameter values needed for the setup of two new pairs of security associations. For further details see 3GPP TS 33.203 [19] and RFC 3329 [48]; and

e) a Security-Verify header field that contains the content of the Security-Server header field received in the 401 (Unauthorized) response of the last successful authentication.

On receiving the 200 (OK) response to the REGISTER request, the UE shall additionally:

a) set the security association lifetime associated with this contact address and the associated set of security associations to the longest of either the previously existing security association lifetime, or the lifetime of the just completed registration plus 30 seconds.

[TS 24.229 clause 5.1.1.5.1]:

On receiving a 401 (Unauthorized) response to the REGISTER request, the UE shall:

1) extract the RAND and AUTN parameters;

2) check the validity of a received authentication challenge, as described in 3GPP TS 33.203 [19] i.e. the locally calculated XMAC must match the MAC parameter derived from the AUTN part of the challenge; and the SQN parameter derived from the AUTN part of the challenge must be within the correct range; and

3) check the existence of the Security-Server header field as described in RFC 3329 [48]. If the Security-Server header field is not present or it does not contain the parameters required for the setup of the set of security associations (see annex H of 3GPP TS 33.203 [19]), the UE shall abandon the authentication procedure and send a new REGISTER request with a new Call-ID.

In the case that the 401 (Unauthorized) response to the REGISTER request is deemed to be valid the UE shall:

1) calculate the RES parameter and derive the keys CK and IK from RAND as described in 3GPP TS 33.203 [19];

2) set up a temporary set of security associations for this registration based on the static list and parameters the UE received in the 401 (Unauthorized) response and its capabilities sent in the Security-Client header field in the REGISTER request. The UE sets up the temporary set of security associations using the most preferred mechanism and algorithm returned by the P-CSCF and supported by the UE and using IK and CK (only if encryption enabled) as the shared key. The UE shall use the parameters received in the Security-Server header field to setup the temporary set of security associations. The UE shall set a temporary SIP level lifetime for the temporary set of security associations to the value of reg-await-auth timer;

3) store the announcement of the media plane security mechanisms the P-CSCF (IMS-ALG) supports received in the Security-Server header field, if any, according to the procedures described in draft-dawes-dispatch-mediasec-parameter [174].

NOTE 1: Security mechanisms that apply to the media plane are distinguished by the "mediasec" header field parameter.

4) send another REGISTER request towards the protected server port indicated in the response using the temporary set of security associations to protect the message. The header fields are populated as defined for the initial REGISTER request that was challenged with the received 401 (Unauthorized) response, with the addition that the UE shall include an Authorization header field containing:

   - the "realm" header field parameter set to the value as received in the "realm" WWW-Authenticate header field parameter;

   - the "username" header field parameter, set to the value of the private user identity;

   - the "response" header field parameter that contains the RES parameter, as described in RFC 3310 [49];

   - the "uri" header field parameter, set to the SIP URI of the domain name of the home network;

   - the "algorithm" header field parameter, set to the value received in the 401 (Unauthorized) response; and

   - the "nonce" header field parameter, set to the value received in the 401 (Unauthorized) response.

   The UE shall also insert the Security-Client header field that is identical to the Security-Client header field that was included in the previous REGISTER request (i.e. the REGISTER request that was challenged with the received 401 (Unauthorized) response). The UE shall also insert the Security-Verify header field into the request, by mirroring in it the content of the Security-Server header field received in the 401 (Unauthorized) response. The UE shall set the Call-ID of the security association protected REGISTER request which carries the authentication challenge response to the same value as the Call-ID of the 401 (Unauthorized) response which carried the challenge.

On receiving the 200 (OK) response for the security association protected REGISTER request registering a public user identity with the associated contact address, the UE shall:

- change the temporary set of security associations to a newly established set of security associations, i.e. set its SIP level lifetime to the longest of either the previously existing set of security associations SIP level lifetime, or the lifetime of the just completed registration plus 30 seconds; and

- if this is the only set of security associations available toward the P-CSCF, use the newly established set of security associations for further messages sent towards the P-CSCF. If there are additional sets of security associations (e.g. due to registration of multiple contact addresses), the UE can either use them or use the newly established set of security associations for further messages sent towards the P-CSCF as appropriate.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.1.4.1, 5.1.1.4.2, 5.1.1.5.1 and 5.1.6.4 (release 9)

19.5.8.3 Test purpose

1) To verify that when half of the time for the emergency registration has expired and the UE is processing a standalone transaction, the UE shall perform user-initiated emergency reregistration, as defined within 3GPP TS 24.229 [10] clauses 5.1.6.4, 5.1.1.4.1, 5.1.1.4.2 and 5.1.1.5.1.

19.5.8.4 Method of test

Initial conditions

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE contains either ISIM and USIM applications or only USIM application on UICC. In the E-UTRA attach SS has indicated to the UE that the cell supports E-UTRA emergency bearers. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step. UE has registered to IMS emergency services, by executing the generic test procedure in Annex C.20 up to the last step with the exception that the SS sets the expiration time to 20 seconds in Step 6. Thereafter the UE has initiated an emergency call by executing the generic test procedure in Annex C.22 up to the last step.

Related ICS/IXIT Statement(s)

- UE supports IMS emergency services (Yes/No)
- IMS security (Yes/No)
- Support for MT SMS over IMS (Yes/No)

Test procedure

1) The emergency call is released on the UE seven seconds after initiating the call. SS waits the UE to send a BYE request.
   Note: It is checked that the release of the emergency call happens within 7 seconds from receipt of the first message of the emergency Call.

2) 9 seconds from receipt of the first message of the IMS Emg Call, and thus one second before half of the emergency registration time has expired, sending of a Mobile Terminating SMS over IMS emergency bearers is initiated at the SS.

2A) The SS waits for the UE to respond to the SIP MESSAGE request with a 200 OK response.

2B) The SS waits for the UE to respond to the SIP MESSAGE request with a delivery report..

3) SS responds to the BYE request with valid 200 OK response.

4) As SS does not respond timer T1 expires and the UE shall resend the SIP MESSAGE request

5) Two seconds after the 2nd SIP MESSAGE request SS responds to the SIP MESSAGE request with a 202 Accepted response.

On parallel, between steps 3) and 5) above, the UE shall initiate the emergency reregistration as described in the parallel behaviour.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		BYE	The UE releases the emergency call with BYE
2	←		SIP MESSAGE request	The SS sends an MT Short Message 9 seconds after initiation of the emergency call.
2A	→		200 OK	The UE responds with 200 OK.
2B	→		SIP MESSAGE request	UE sends a SIP MESSAGE request including a vnd.3gpp.sms payload that contains a short message delivery report.
3	←		200 OK	The SS sends 200 OK for BYE
4	→		SIP MESSAGE request	UE resends the SIP MESSAGE request after the timeout as SS did not send a reply
5	←		202 Accepted	SS responds with 202 Accepted one second after the second SIP MESSAGErequest

Expected sequence, parallel behaviour

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	UE re-registers to the emergency services 10 seconds before the expected expiration.
2	←		401 Unauthorized	The SS responds with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network.
3	→		REGISTER	UE completes the security negotiation procedures, sets up a new temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials.
4	←		200 OK	The UE responds with 200 OK.

Specific Message Contents

BYE (Step 1)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE (Step 3)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

SIP MESSAGE request (Steps 2)

Use the default message 'Message for MT SMS' in Annex A.7.1

200 OK for BYE (Step 2A)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

SIP MESSAGE request (Step 2B)

Use the default message 'Message for delivery report' in Annex A.7.2

202 Accepted for SIP MESSAGE request (Step 5)

Use the default message '202 Accepted' in annex A.3.3.

Specific Message Contents for parallel behaviour

REGISTER (Step 1)

Use the default message 'REGISTER' in annex A.1.1. with condition A2 "Subsequent REGISTER sent over security associations' and the following exceptions applying:

Header/param	Value/remark
Contact	
addr-spec	SIP URI with IP address or FQDN and protected server port of UE. The SIP URI shall contain the *sos* URI parameter.
Security-Client	
spi-c	new SPI number of the inbound SA at the protected client port
spi-s	new SPI number of the inbound SA at the protected server port
port-c	new protected client port needed for the setup of new pairs of security associations
port-s	Same value as in the previous REGISTER

401 Unauthorized for REGISTER (Step 2)

Use the default message '401 Unauthorized for REGISTER' in annex A.1.2 with the following exceptions:

Header/param	Value/remark
Security-Server	
spi-c	new SPI number of the inbound SA at the protected client port
spi-s	new SPI number of the inbound SA at the protected server port
port-c	new protected client port needed for the setup of new pairs of security associations
port-s	Same value as in the previous Security-Server headers
WWW-Authenticate	
nonce	Base 64 encoding of a new RAND and AUTN

REGISTER (Step 3)

Use the default message 'REGISTER' in annex A.1.1 like in step 1 above. The only difference is that the response value within Authorization header shall have been recalculated based on the nonce received from SS within 401 response.

200 OK for REGISTER (Step 4)

Use the default message '200 OK for REGISTER' in annex A.1.3 with condition A3 'Response for an emergency registration' and the expires parameter of Contact header set to 1200.

19.5.8.5 Test requirements

All the messages specified for this test case shall be sent over the EPS emergency bearers allocated for the initial emergency registration.

19.5.9 In parallel emergency and non-emergency registrations

19.5.9.1 Definition and applicability

Test to verify that the UE handles the IMS emergency registration and related signalling independently from any other ongoing IMS registration.

19.5.9.2 Conformance requirement

[TS 24.229 clause 5.1.6.2]:

When the UE performs an initial emergency registration and whilst this emergency registration is active, the UE shall:

- handle the emergency registration independently from any other ongoing registration to the IM CN subsystem;
- handle any signalling or media related IP-CAN for the purpose of emergency calls independently from any other established IP-CAN for IM CN subsystem related signalling or media; and
- handle all SIP signalling and all media related to the emergency call independently from any other ongoing IM CN subsystem signalling and media.

Reference(s)

3GPP TS 24.229[10], clause 5.1.6.2 (release 9)

19.5.9.3 Test purpose

1) To verify that the UE maintains the emergency call even if the network would initiate the deregistration procedure for the non-emergency IMS registration

19.5.9.4 Method of test

Initial conditions

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

Related ICS/IXIT Statement(s)

- UE supports IMS emergency services (Yes/No)
- IMS security (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-15) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 15 for EPS emergency bearer context activation, IMS emergency registration and subsequent IMS emergency speech call

16) SS sends a SIP NOTIFY request in order to terminate the non-emergency IMS registration.

17) UE responds the NOTIFY request with 200 OK response. The emergency call remains unaffected on the UE.

18) Emergency call is terminated manually on the UE. Consequently the UE sends SIP BYE request.

19) SS responds the BYE request with 200 OK response.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-15			Steps defined in annex C.20 followed by the steps defined in annex C.22	IMS emergency registration by the UE followed by IMS emergency call setup with PSAP. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
16	←		NOTIFY	The SS sends a NOTIFY for registration event package, containing partial registration state information, with all previously registered non-emergency public user identities as "terminated" and "rejected"
17	→		200 OK	The UE responds the NOTIFY with 200 OK
18	→		BYE	The UE releases the emergency call with BYE
19	←		200 OK	The SS sends 200 OK for BYE

Specific Message Contents

NOTIFY (Step 16)

Use the default message 'NOTIFY for reg-event package' in annex A.1.6 with the following exceptions:

Header/param	Value/remark
CSeq Value	 2
Message-body	*<?xml version='1.0?>* *<reginfo xmlns='urn:ietf:params:xml:ns:reginfo' version='1' state='partial'>* *<registration aor=*'PublicUserIdentity2 (NOTE 1)' *id='a102' state='terminated'>* *<contact id='980' state='terminated' event='rejected'>* <*uri*>same value as in Contact header of REGISTER request*</uri>* *</contact>* *</registration>* *<registration aor=*'AssociatedTelUri(NOTE 1)' *id='a101' state='terminated'>* *<contact id='981' state='terminated' event='rejected'>* <*uri*>same value as in Contact header of REGISTER request*</uri>* *</contact>* *</registration>* *</reginfo>*

NOTE 1: The public user ids and the associated TEL URI are as returned to the UE in the P-Associated-URI header of the 200 (OK) response to the REGISTER request;
PublicUserId1 is the default public user id i.e. the first one contained in P-Associated-URI;
AssociatedTelUri is the same as used in P-Associated-URI
PublicUserId2 and PublicUserId3 are the remaining IMPUs of the P-Associated-URI header

200 OK for NOTIFY (Step 17)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

BYE (Step 18)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE (Step 19)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

19.5.9.5 Test requirements

UE maintains the IMS emergency call even if the non-emergency IMS registration is terminated by the SS.

19.5.10 Deregistration upon emergency registration expiration

19.5.10.1 Definition and applicability

Test to verify that when there is no emergency call going on or being set up, neither there are any standalone transactions related to the IMS emergency registration when half of the time for IMS emergency registration has expired, the UE will not extend the IMS emergency registration but instead silently wait for the emergency registration to expire.

19.5.10.2 Conformance requirement

[TS 24.229 clause 5.1.6.4]:

The UE shall perform user-initiated emergency reregistration as specified in subclause 5.1.1.4 if half of the time for the emergency registration has expired and:

- the UE has emergency related ongoing dialog; or
- standalone transactions exist; or
- the user initiates an emergency call.

The UE shall not perform user-initiated emergency reregistration in any other cases.

[TS 24.229 clause 5.1.6.6]:

Once the UE registers a public user identity and an associated contact address via emergency registration, the UE shall not perform user-initiated deregistration of the respective public user identity and the associated contact address.

NOTE: The UE will be deregistered when the emergency registration expires.

Reference(s)

3GPP TS 24.229[10], clauses 5.1.6.4 and 5.1.6.6

19.5.10.3 Test purpose

1) To verify that the UE will not reregister to IMS emergency services in the absence of emergency related dialog, standalone transaction or emergency call initiation.

19.5.10.4 Method of test

Initial conditions

SS is configured with the IMSI within the USIM application, the home domain name, public and private user identities (including the public emergency user identity allocated for the user) together with the shared secret key of IMS AKA algorithm, related to the IMS private user identity (IMPI) that is configured on the UICC card equipped into the UE. SS is listening to SIP default port 5060 for both UDP and TCP protocols. SS is able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [14] clause 6.1 and RFC 3310 [17].

UE contains either ISIM and USIM applications or only USIM application on UICC. UE is registered to IMS services, by executing the generic test procedure in Annex C.2 up to the last step.

Related ICS/IXIT Statement(s)

- UE supports IMS emergency services (Yes/No)
- IMS security (Yes/No)

Test procedure applicable for a UE with E-UTRA support (TS 34.229-2 [5] A.18/1)

1-15) UE executes the procedures described in TS 36.508 [94] table 4.5A.4.3-1 steps 1 to 15 for EPS emergency bearer context activation, IMS emergency registration and subsequent IMS emergency speech call. As an exception the SS sets the expiration time to 100 seconds in Step 6 of Annex C.20.

16) The emergency call is terminated on the UE 20 seconds after it has been initiated. UE sends SIP BYE request.

17) SS responds BYE with 200 OK response.

Expected sequence

NOTE: Only the IMS procedure relevant to the test purpose is described below.

Step	Direction		Message	Comment
	UE	SS		
1-15			Steps defined in annex C.20 followed by the steps defined in annex C.22	IMS emergency registration by the UE followed by IMS emergency call setup with PSAP. Referred from 36.508 [94] table 4.5A.4.3-1 for a UE with E-UTRA support.
16	→		BYE	When the emergency call is terminated on the UE, the UE sends BYE to release the emergency call.
17	←		200 OK	The SS sends 200 OK for the BYE request and ends the call.

BYE (step 16)

Use the default message "BYE" in annex A.2.8.

200 OK (step 17)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

19.5.10.5 Test requirements

The UE shall not send IMS emergency reregistration within 110 seconds from the IMS emergency registration done within step 1.

Annex A (normative): Default Messages

For all the message definitions below, the acceptable order and syntax of headers and fields within these headers must be according to IETF RFCs where those headers have been defined. Typically the order of headers is not significant, but there are well defined exceptions (like Via, Route Record-Route headers and SDP lines) where the order is important.

The contents of the messages described in the present Annex is not complete - only the fields headers and SDP lines required to be checked or generated by SS are listed here. The messages sent by the UE may contain additional parameters, fields headers and SDP lines which are not checked and must thus be ignored by SS.

Values prefixed with px_ will be implemented in the TTCN with a PIXIT.

Values shown in *italics* shall be used in the messages as such.

A.1 Default messages for IMS Registration

A.1.1 REGISTER

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*REGISTER*		
Request-URI		SIP URI formed from home domain name as stored in EF_{DOMAIN} (when using ISIM) or SIP URI formed from home domain name derived from the IMSI (when no ISIM available on the UICC)		
SIP-Version		*SIP/2.0*		
Route		**Not present**		RFC 3261 [15]
Via				RFC 3261 [15] RFC 3581 [96]
sent-protocol		*SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP)		
sent-by	A1, A3	IP address or FQDN, port (optional) and not checked		
sent-by	A2	IP address or FQDN and protected server port of the UE		
via-branch		value starting with "*z9hG4bK*"		
response-port	A1, A3	*rport (when using UDP)*		
From				RFC 3261 [15]
addr-spec	A1	any IMPU within the set of IMPUs on ISIM (when using ISIM; NOTE 3) or public user identity derived from IMSI (when no ISIM available on the UICC)		
addr-spec	A2	same public user identity as in initial REGISTER		
addr-spec	A3	public user identity derived from IMSI		
addr-spec	A7	emergency public user identity (NOTE 4)		
tag		must be present, value not checked		
To				RFC 3261 [15]
addr-spec	A1,-	any IMPU within the set of IMPUs on ISIM (when using ISIM; NOTE 3) or public user identity derived from IMSI (when no ISIM available on the UICC)		
addr-spec	A2	same public user identity as in initial REGISTER		
addr-spec	A3	public user identity derived from IMSI		
addr-spec	A7	emergency public user identity (NOTE 4)		
tag		must not be present		
Contact				RFC 3261 [15] RFC 5627 [61]
addr-spec	A1, A3	SIP URI with IP address or FQDN and indicating either an unprotected port selected by the UE or no port at all. When A7 the SIP URI shall contain the *sos* URI parameter.		
addr-spec	A2	SIP URI with IP address or FQDN and protected server port of UE. When A7 the SIP URI shall contain the *sos* URI parameter.		
feature-param	A4	*+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"* (see NOTE 2)		
feature-param	A6	*+g.3gpp.smsip*		
feature-param	A10	*video*		
c-p-instance	A5	+sip.instance media feature tag with the instance ID of the UE	Rel-10	draft-montemurro-gsma-imei-urn-19 [122]
expires		*600000* (if present)		
Expires		**(if present)**		RFC 3261 [15]
delta-seconds		*600000*		
Require	A1, A2			RFC 3261 [15] RFC 3329 [21]
option-tag		*sec-agree*		
Proxy-Require	A1, A2			RFC 3261 [15] RFC 3329 [21]
option-tag		*sec-agree*		
Supported				RFC 3261 [15]

Header/param	Cond	Value/remark	Rel	Reference
option-tag	A5	*gruu*		
option-tag		*path*		
CSeq				RFC 3261 [15]
value	A1, A3	must be present, value not checked		
value	A2	must be incremented from the previous REGISTER		
method		*REGISTER*		
Call-ID				RFC 3261 [15]
callid		value not checked		
Session-ID	A8			draft-kaplan-dispatch-session-id [115]
sess-id		value not checked		
Security-Client	A1, A2			RFC 3329 [21]
mechanism-name		*ipsec-3gpp*		
algorithm		*hmac-md5-96*		
protocol		*esp* (if present)		
mode		*trans* (if present)		
encrypt-algorithm		***des-ede3-cbc*** or ***aes-cbc***		
spi-c		SPI number of the inbound SA at the protected client port		
spi-s		SPI number of the inbound SA at the protected server port		
port-c		protected client port		
port-s		protected server port		
mechanism-name		*ipsec-3gpp*		
algorithm		*hmac-sha-1-96*		
protocol		*esp* (if present)		
mode		*trans* (if present)		
encrypt-algorithm		***des-ede3-cbc*** or ***aes-cbc***		
spi-c		SPI number of the inbound SA at the protected client port		
spi-s		SPI number of the inbound SA at the protected server port		
port-c		protected client port		
port-s		protected server port		
Security-Verify	A2	(not present when A1, A3)		RFC 3329 [21]
sec-mechanism	A2	same value as SecurityServer header sent by SS		
Authorization	A1			RFC 2617 [16]
username	A1	private user identity as stored in EF_{IMPI} (when using ISIM) or private user identity derived from IMSI (when no ISIM available on the UICC)		RFC 3310 [17]
realm	A1	home domain name as stored in EF_{DOMAIN} (when using ISIM) or home domain name derived from the IMSI (when no ISIM available on the UICC)		
nonce	A1	set to an empty value		
digest-uri	A1	SIP URI formed from home domain name as stored in EF_{DOMAIN} (when using ISIM) or formed from home domain name derived from the IMSI (when no ISIM available on the UICC)		
response	A1	set to an empty value		
Authorization	A2			RFC 2617 [16]
username	A2	private user identity as stored in EF_{IMPI} (when using ISIM) or private user identity derived from IMSI (when no ISIM available on the UICC)		RFC 3310 [17]
realm	A2	same value as received in the realm directive in the WWW Authenticate header sent by SS		
nonce	A2	same value as in WWW-Authenticate header sent by SS		
opaque	A2	same value as sent by the server in '401 Unauthorized for REGISTER'		
digest-uri	A2	SIP URI formed from home domain name as stored in EF_{DOMAIN} (when using ISIM) or formed from home domain name derived from the IMSI (when no ISIM available on the UICC)		
qop-value	A2	*auth*		

Header/param	Cond	Value/remark	Rel	Reference
cnonce-value	A2	value assigned by UE affecting the response calculation		
nonce-count	A2	counter to indicate how many times UE has sent the same value of nonce within successive REGISTERs, initial value shall be 1		
response	A2	response calculated by UE		
algorithm	A2	*AKAv1-MD5*		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
P-Access-Network-Info	A2	(header optional when A1, A3)		RFC 3455 [18]
access-net-spec	A2	access network technology and, if applicable, the cell ID		
Content-Length				RFC 3261 [15]
value		length of request body, if such is present		

Condition	Explanation
A1	Initial unprotected REGISTER (IMS security, A.6a/2 3GPP TS 34.229-2 [5])
A2	Subsequent REGISTER sent over security associations (IMS security, A.6a/2 3GPP TS 34.229-2 [5])
A3	REGISTER for the case UE supports GIBA (A.6a/1 3GPP TS 34.229-2 [5])
A4	The UE supports IMS Multimedia Telephony (MTSI) (A.3A/50 3GPP TS 34.229-2 [5])
A5	obtaining and using GRUUs in the Session Initiation Protocol (SIP) (A.4/53 3GPP TS 34.229-2 [5]). Mandatory from Rel-10 onwards.
A6	The UE supports SM-over-IP receiver (A.3A/62 3GPP TS 34.229-2 [5])
A7	Initial IMS emergency registration
A8	UE supports Session-ID (A.12/30 3GPP TS 34.229-2 [5])
A10	UE indicates video media feature tag in REGISTER and INVITE request (A.12/32 3GPP TS 34.229-2 [5])

NOTE 1: All choices for applicable conditions are described for each header.

NOTE 2: The '=' may include optional linear white spaces according to the EQUAL definition in chapter 25.1, RFC 3261 [15].

NOTE 3: Public user identity shall be the same for "From" and "To".

NOTE 4: According to TS 24.229 clause 5.1.1.1A and 5.1.6.2 [10] when the UE is using ISIM the emergency public user identity is the first public user identity in the list stored in the ISIM; when there is no ISIM it is the default public user id if the UE non-emergency registered with the IM CN and the temporary user id (derived from IMSI) in all other cases.

A.1.2 401 Unauthorized for REGISTER

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 3261 [15]
SIP-Version	*SIP/2.0*		
Status-Code	*401*		
Reason-Phrase	*Unauthorized*		
Via			RFC 3261 [15]
via-parm	same value as received in REGISTER message		
To			RFC 3261 [15]
addr-spec	same value as received in REGISTER message		
tag	common to-tag (register)		
From			RFC 3261 [15]
addr-spec	same value as received in REGISTER message		
tag	same value as received in REGISTER message		
Call-ID			RFC 3261 [15]
callid	same value as received in REGISTER message		
Session-ID			draft-kaplan-dispatch-session-id [115]
sess-id	same value as received in REGISTER message, if Session-ID header field exists in received REGISTER message, otherwise, not present.		
CSeq			RFC 3261 [15]
value	same value as received in REGISTER message		
WWW-Authenticate			RFC 2617 [16] RFC 3310 [17]
realm	home domain name as stored in EF_{DOMAIN} or home domain name derived from the IMSI		
algorithm	*AKAv1-MD5*		
qop-value	*auth*		
nonce	Base 64 encoding of RAND and AUTN		
opaque	arbitrary value (to be returned by the UE in subsequent REGISTER)		
Security-Server			RFC 3329 [21]
mechanism-name	*ipsec-3gpp*		
algorithm	px_IpSecAlgorithm (hmac-md5-96 or hmac-sha-1-96)		
spi-c	SPI number of the inbound SA at the protected client port		
spi-s	SPI number of the inbound SA at the protected server port		
port-c	protected client port of SS		
port-s	protected server port of SS		
Encrypt-algorithm	des-ede3-cbc or aes-cbc		
q	0.9		
Mechanism-name	Ipsec-3gpp		
algorithm	Algorithm not selected by px_IpSecAlgorithm (hmac-sha-1-96 or hmac-md5-96)		
spi-c	SPI number of the inbound SA at the protected client port		
spi-s	SPI number of the inbound SA at the protected server port		
port-c	protected client port of SS		
port-s	protected server port of SS		
encrypt-algorithm	des-ede3-cbc or aes-cbc		
q	0.7		
Content-Length			RFC 3261 [15]
value	0		

A.1.3 200 OK for REGISTER

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*200*		
Reason-Phrase		*OK*		
Via				RFC 3261 [15]
via-parm		same value as received in REGISTER message		
To				RFC 3261 [15]
addr-spec		same value as received in REGISTER message		
tag		common to-tag (register)		
From				RFC 3261 [15]
addr-spec		same value as received in REGISTER message		
tag		same value as received in REGISTER message		
Call-ID				RFC 3261 [15]
callid		same value as received in REGISTER message		
Session-ID				draft-kaplan-dispatch-session-id [115]
sess-id		same value as received in REGISTER message, if Session-ID header field exists in received REGISTER message, otherwise, not present.		
CSeq				RFC 3261 [15]
value		same value as received in REGISTER message		
Contact				RFC 3261 [15] RFC 5627 [61]
addr-spec		same value as received in REGISTER message		
pub-gruu	A1	Public GRUU as the SIP URI got from the To header of the REGISTER request, together with the gr parameter with an arbitrary value		
temp-gruu	A1	Temporary GRUU with an arbitrary value in the user part and the host part matching with the domain of the To header of the REGISTER and gr parameter without any value (temp-gruu parameter missing when A3)		
feature-param		same value as received in REGISTER message		
expires		600		
P-Associated-URI		order of the parameters in this header must be like in this table		RFC 3455 [18]
addr-spec	A2	all the IMPUs within the set of IMPUs on ISIM (NOTE 1)		
addr-spec	A2	additional associated TEL URI (NOTE2)		
addr-spec	A3	emergency public user identity (NOTE 3)		
Service-Route		(header missing when A3)		RFC 3608 [19]
addr-spec	A2	px_scscf		
uri-parameter		*lr*		
Path				RFC 3327 [20]
addr-spec		px_pcscf		
uri-parameter		*lr*		
Content-Length				RFC 3261 [15]
value		0		

Condition	Explanation
A1	obtaining and using GRUUs in the Session Initiation Protocol (SIP) (A.4/53 3GPP TS 34.229-2 [5])
A2	Response for an non-emergency registration
A3	Response for an emergency registration

NOTE 1: The set of IMPUs shall be in accordance to annex E.3 independent of whether the UE has an ISIM on the UICC or not (i.e. when the UE has no ISIM SS shall use the same values as if the UE would have an ISIM; furthermore in this case the temporary public user id shall not be included in the set of IMPUs)

NOTE 2: any arbitrary (but valid) TEL URI

NOTE 3: According to TS 24.229 clause 5.1.1.1A and 5.1.6.2 [10] when the UE is using ISIM the emergency public user identity is the first public user identity in the list stored in the ISIM; when there is no ISIM it is the default public user id if the UE non-emergency registered with the IM CN and the temporary user id (derived from IMSI) in all other cases.

A.1.4 SUBSCRIBE for reg-event package

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*SUBSCRIBE*		
Request-URI		Public user identity used for subscription (NOTE 2)		
SIP-Version		*SIP/2.0*		
Route		order of the parameters in this header must be like in this table		RFC 3261 [15]
route-param	A1	<*sip:*px_pcscf:protected server port of P-CSCF;*lr*>, <*sip:*px_scscf;*lr*>		
route-param	A2	<*sip:*px_pcscf: unprotected server port of P-CSCF (optional);*lr*>, <*sip:*px_scscf;*lr*>		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by	A1	IP address or FQDN and protected server port of the UE		
sent-by	A2	IP address or FQDN, port (optional) and not checked		
via-branch		value starting with "*z9hG4bK"*		
From				RFC 3261 [15]
addr-spec		Public user identity used for subscription (NOTE 2		
tag		must be present, value not checked but stored for later reference		
To				RFC 3261 [15]
addr-spec		Public user identity used for subscription (NOTE 2		
tag		must not be present		
Contact				RFC 3261 [15]
addr-spec	A1	SIP URI with IP address or FQDN and protected server port of UE or GRUU as returned by the SS in registration		
addr-spec	A2	SIP URI with IP address or FQDN and unprotected server port of UE or GRUU as returned by the SS in registration		
Expires				RFC 3261 [15]
delta-seconds		*600000*		
Security-Verify	A1			RFC 3329 [21]
sec-mechanism		same value as SecurityServer header sent by SS		
Require	A1			RFC 3261 [15]
option-tag		*sec-agree*		RFC 3329 [21]
Proxy-Require	A1			RFC 3261 [15]
option-tag		*sec-agree*		RFC 3329 [21]
CSeq				RFC 3261 [15]
value		must be present, value not checked		
method		*SUBSCRIBE*		
Call-ID				RFC 3261 [15]
callid		value not checked, but stored for later reference		
Session-ID	A3			draft-kaplan-dispatch-session-id [115]
sess-id		value not checked, but stored for later reference		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
P-Access-Network-Info	A1	(header optional when A2)		RFC 3455 [18]
access-net-spec		access network technology and, if applicable, the cell ID		
Accept		**(if present)**		RFC 3261 [15]
media-range		*application/reginfo+xml*		RFC 3680 [22]
Event				RFC 3265 [34]
event-type		*reg*		RFC 3680 [22]
Content-Length				RFC 3261 [15]
value		length of request body, if such is present		

Condition	Explanation
A1	IMS security (A.6a/2 3GPP TS 34.229-2 [5])

A2	GIBA (A.6a/1 3GPP TS 34.229-2 [5])
A3	UE supports Session-ID (A.12/30 3GPP TS 34.229-2 [5])

NOTE1: All choices for applicable conditions are described for each header.

NOTE2: According to TS 24.229 clause 5.1.1.3 the public user identity used for subscription is:
a) when the UE has an ISIM the default public user identity or the public user identity used for initial registration
b) when the UE does not have an ISIM the default public user identity

A.1.5 200 OK for SUBSCRIBE

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*200*		
Reason-Phrase		*OK*		
Via				RFC 3261 [15]
via-parm		same value as received in SUBSCRIBE message		
To				RFC 3261 [15]
addr-spec		same value as received in SUBSCRIBE message		
tag		common to-tag (subscribe dialog)		
From				RFC 3261 [15]
addr-spec		same value as received in SUBSCRIBE message		
tag		same value as received in SUBSCRIBE message		
Call-ID				RFC 3261 [15]
callid		same value as received in SUBSCRIBE message		
CSeq				RFC 3261 [15]
value		same value as received in SUBSCRIBE message		
Contact				RFC 3261 [15]
addr-spec		<*sip:*px_scscf>		
Expires				RFC 3261 [15]
delta-seconds		600000		
Record-Route				RFC 3261 [15]
addr-spec	A1	px_pcscf: protected server port of SS		
addr-spec	A2	px_pcscf: unprotected server port of SS (optional)		
uri-parameter		lr		
Content-Length				RFC 3261 [15]
value		0		

Condition	Explanation
A1	IMS security (A.6a/2 3GPP TS 34.229-2 [5])
A2	GIBA (A.6a/1 3GPP TS 34.229-2 [5])

NOTE1: All choices for applicable conditions are described for each header.

A.1.6 NOTIFY for reg-event package

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*NOTIFY*		
Request-URI	A1	same URI as used by the UE in the corresponding REGISTER message and protected server port of UE		
Request-URI	A2	same URI as used by the UE in the corresponding REGISTER message and unprotected server port of UE		
SIP-Version		*SIP/2.0*		
Via		order of the parameters in this header must be like in this table		RFC 3261 [15]
via-parm1:				
Sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by	A1	IP address and protected server port of SS		
sent-by	A2	IP address and unprotected server port of SS (optional)		
via-branch		value starting with "*z9hG4bK"*		
via-parm2:				
sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by		px_scscf		
via-branch		value starting with "*z9hG4bK"*		
From				RFC 3261 [15]
addr-spec		same URI as received in the To header of the previous SUBSCRIBE message (NOTE 3)		
tag		common to-tag (subscribe dialog)		
To				RFC 3261 [15]
addr-spec		same URI as received in the From header of the previous SUBSCRIBE message (NOTE 3)		
tag		same value as received in From tag of SUBSCRIBE message		
Call-ID				RFC 3261 [15]
callid		same as value received in SUBSCRIBE message		
CSeq	A1,A2			RFC 3261 [15]
value		1		
method		*NOTIFY*		
Contact				RFC 3261 [15]
addr-spec		<*sip:*px_scscf>		
Content-Type				RFC 3261 [15]
media-type		*application/reginfo+xml*		RFC 3680 [22]
Event	A1,A2			RFC 3265[34]
event-type		*reg*		RFC 3680 [22]
Max-Forwards				RFC 3261 [15]
value		*69*		
Subscription-State				RFC 3265[34]
substate-value		*active*		
expires		*600000*		
Content-Length				RFC 3261 [15]
value		length of message-body		RFC 3680 [22]
Message-body	A3	<?xml version='1.0?> <reginfo xmlns='urn:ietf:params:xml:ns:reginfo' version='0' state='full'> <registration aor='PublicUserIdentity1 (NOTE 2)' id='a100' state='active'> <contact id='980' state='active' event='registered'> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> <registration aor='AssociatedTelUri (NOTE 2)' id='a101' state='active'> <contact id='981' state='active' event='created'> <uri>same value as in Contact header of REGISTER request</uri> </contact>		

Header/param	Cond	Value/remark	Rel	Reference
		</registration> <registration aor='PublicUserIdentity2 (NOTE 2)' id='a102' state='active'> <contact id='982' state='active' event='registered'> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> <registration aor='PublicUserIdentity3 (NOTE 2)' id='a103' state='active'> <contact id='983' state='active' event='registered'> <uri>same value as in Contact header of REGISTER request</uri> </contact> </registration> </reginfo>		
	A4	<?xml version='1.0?> <reginfo xmlns='urn:ietf:params:xml:ns:reginfo' xmlns:gr="urn:ietf:params:xml:ns:gruuinfo" version='0' state='full'> <registration aor='PublicUserIdentity1 (NOTE 2)' id='a100' state='active'> <contact id='980' state='active' event='registered' callid="Call-Id of most recent REGISTER" cseq="CSeq value of most recent REGISTER"> <uri>same value as in Contact header of REGISTER request</uri> <allOneLine> <unknown-param name="+sip.instance"> "Instance ID of the UE;" </unknown-param> </allOneLine> <allOneLine> <gr:pub-gruu uri="public GRUU for the UE"/> </allOneLine> <allOneLine> <gr:temp-gruu uri="temporary GRUU for the UE" first-cseq="CSeq of the REGISTER request that caused the temporary GRUU to assigned for the UE"/> </allOneLine> </contact> </registration> <registration aor='AssociatedTelUri (NOTE 2)' id='a101' state='active'> <contact id='981' state='active' event='created'> <uri>same value as in Contact header of REGISTER request</uri> <allOneLine> <unknown-param name="+sip.instance"> "Instance ID of the UE;" </unknown-param> </allOneLine> <allOneLine> <gr:pub-gruu uri="public GRUU for the UE"/> </allOneLine> <allOneLine> <gr:temp-gruu uri="temporary GRUU for the UE" first-cseq="CSeq of the REGISTER request that caused the temporary GRUU to assigned for the UE"/> </allOneLine> </contact> </registration> <registration aor='PublicUserIdentity2 (NOTE 2)' id' id='a102' state='active'> <contact id='982' state='active' event='registered' callid="Call-Id of most recent REGISTER" cseq="CSeq value of most recent REGISTER">		RFC5628[62]

Header/param	Cond	Value/remark	Rel	Reference
		<uri>same value as in Contact header of REGISTER request</uri> <allOneLine> <unknown-param name="+sip.instance"> "Instance ID of the UE;" </unknown-param> </allOneLine> <allOneLine> <gr:pub-gruu uri="public GRUU for the UE"/> </allOneLine> <allOneLine> <gr:temp-gruu uri="temporary GRUU for the UE" first-cseq="CSeq of the REGISTER request that caused the temporary GRUU to assigned for the UE"/> </allOneLine> </contact> </registration> <registration aor='PublicUserIdentity3 (NOTE 2)' id' id='a103' state='active'> <contact id='983' state='active' event='registered' callid="Call-Id of most recent REGISTER" cseq="CSeq value of most recent REGISTER"> <uri>same value as in Contact header of REGISTER request</uri> <allOneLine> <unknown-param name="+sip.instance"> "Instance ID of the UE;" </unknown-param> </allOneLine> <allOneLine> <gr:pub-gruu uri="public GRUU for the UE"/> </allOneLine> <allOneLine> <gr:temp-gruu uri="temporary GRUU for the UE" first-cseq="CSeq of the REGISTER request that caused the temporary GRUU to assigned for the UE"/> </allOneLine> </contact> </registration> </reginfo>		

Condition	Explanation
A1	IMS security (A.6a/2 3GPP TS 34.229-2 [5])
A2	GIBA (A.6a/1 3GPP TS 34.229-2 [5]
A3	NOT obtaining and using GRUUs in the Session Initiation Protocol (SIP) (A.4/53 3GPP TS 34.229-2 [5])
A4	obtaining and using GRUUs in the Session Initiation Protocol (SIP) (A.4/53 3GPP TS 34.229-2 [5])

NOTE 1: All choices for applicable conditions are described for each header.

NOTE 2: The public user ids and the associated TEL URI are as returned to the UE in the P-Associated-URI header of the 200 (OK) response to the REGISTER request;
PublicUserId1 is the default public user id i.e. the first one contained in P-Associated-URI;
AssociatedTelUri is the same as used in P-Associated-URI
PublicUserId2 and PublicUserId3 are the remaining IMPUs of the P-Associated-URI header

NOTE 3: This results in using the public user identity used for subscription as defined in TS 24.229 clause 5.1.1.3.

A.1.7 423 Interval Too Brief for REGISTER

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 3261 [15]
SIP-Version	*SIP/2.0*		
Status-Code	*423*		
Reason-Phrase	*Interval Too Brief*		
Via			RFC 3261 [15]
via-parm	same value as received in REGISTER message		
To			RFC 3261 [15]
addr-spec	same value as received in REGISTER message		
tag	common to-tag (register)		
From			RFC 3261 [15]
addr-spec	same value as received in REGISTER message		
Call-ID			RFC 3261 [15]
callid	same value as received in REGISTER message		
Session-ID			draft-kaplan-dispatch-session-id [115]
sess-id	same value as received in REGISTER message, if Session-ID header field exists in received REGISTER message, otherwise, not present.		
CSeq			RFC 3261 [15]
value	same value as received in REGISTER message		
Min-Expires			RFC 3261 [15]
delta-seconds	*T (a decimal integer number of seconds from 0 to (2**32)-1)*		

A.1.8 420 Bad Extension for REGISTER

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 3261 [15]
SIP-Version	*SIP/2.0*		
Status-Code	*420*		
Reason-Phrase	*Bad Extension*		
Via			RFC 3261 [15]
via-parm	same value as received in REGISTER message		
To			RFC 3261 [15]
addr-spec	same value as received in REGISTER message		
tag	common to-tag (register)		
From			RFC 3261 [15]
addr-spec	same value as received in REGISTER message		
Call-ID			RFC 3261 [15]
callid	same value as received in REGISTER message		
Session-ID			draft-kaplan-dispatch-session-id [115]
sess-id	same value as received in REGISTER message, if Session-ID header field exists in received REGISTER message, otherwise, not present.		
CSeq			RFC 3261 [15]
value	same value as received in REGISTER message		
Unsupported			RFC 3261 [15]
option-tag	*sec-agree*		

A.2 Default messages for Call Setup

A.2.1 INVITE for MO Call Setup

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15] RFC 5031 [97] TS 24.229 [10] 5.1.2A.1.3, 5.1.2A.1.5, 7.2A.10
Method		*INVITE*		
Request-URI	A4	Px_CalleeUri px_CalleeURI may be either SIP or Tel URI. It may contain a dialstring and phone-context parameter, when calling to dialstring. When calling to dialstring SIP URI must also contain user=phone or user=dialstring parameter. The dialstring, if used, may be global, home local number or geo-local number. For home local numbers the value of phone-context parameter must equal the home domain name i.e. px_HomeDomainName. For geo-local numbers the home domain name must be prefixed by string 'geo-local.' or access technology specific prefix, if the UE supports that option. Note: The way how the UE determines whether numbers in a non-international format are geo-local, home-local or relating to another network, is UE implementation specific. For instance the UE might have a UI setting.		
Request-URI	A5	px_CalleeContactUri		
Request-URI	A6, A7	emergency service URN beginning as *urn:service:sos*		
SIP-Version		*SIP/2.0*		
Via				RFC 3261 [15] RFC 3581 [96]
sent-protocol		*SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP)		
sent-by	A1, A7	IP address or FQDN and protected server port of the UE		
	A2	IP address or FQDN, port (optional) and not checked		
	A6	IP address and unprotected server port of the UE		
response-port	A6	*rport (when using UDP)*		
via-branch		value starting with "*z9hG4bK"*		
Route		order of the parameters in this header must be like in this table		RFC 3261 [15]
route-param	A1	<*sip:*px_pcscf: protected server port of SS *;lr>,* <*sip:*px_scscf;*lr*>		
	A2	<*sip:*px_pcscf: unprotected server port of SS (optional)*;lr>,* <*sip:*px_scscf;*lr*		
	A6	<*sip:*px_pcscf: unprotected server port of SS >		
	A7	<*sip:*px_pcscf: protected server port of SS >		
From				RFC 3261 [15]
addr-spec	A6	Any SIP URI with display name as '*Anonymous'*		
	A7	emergency public user identity (NOTE 3)		
	A4	any SIP URI being subscribed and registered as listed in the XML body of the NOTIFY request; additionally when there is a P-Preferred-Identity header within the INVITE request the SIP URI shall match the URI within the P-Preferred-Identity header		
tag	A4	must be present, value not checked		
addr-spec	A5	local SIP URI of the UE as used in any previous request in the same dialog (In the earlier requests within the same dialog this URI appears in From header within requests sent by the UE and in To header within requests sent by the SS)		
tag	A5	local tag value corresponding to the SIP URI of the UE in the same dialog. (In the earlier requests within the same dialog this tag appears in From header within requests sent by the UE and in To header within requests sent by the SS)		

Header/param	Cond	Value/remark	Rel	Reference
To				RFC 3261 [15] RFC 5031 [97]
addr-spec	A6, A7	emergency service URN beginning as *urn:service:sos*		
addr-spec	A4	px_CalleeUri		
tag	A4	not present		
addr-spec	A5	remote SIP URI of SS (i.e. the remote UE) as used in any previous request in the same dialog (In the earlier requests within the same dialog this URI appears in To header within requests sent by the UE and in From header within requests sent by the SS)		
tag	A5	remote tag value corresponding to the SIP URI of the SS in the same dialog. (In the earlier requests within the same dialog this tag appears in To header within requests sent by the UE and in From header within requests sent by the SS)		
Call-ID				RFC 3261 [15]
callid	A4	value different to that received in REGISTER message		
callid	A5	value of Call-ID as in any previous request in the same dialog		
Session-ID		(header exists when A9)		draft-kaplan-dispatch-session-id [115]
sess-id	A4	value different to that received in REGISTER message		
sess-id	A5	value of Session-ID as in any previous request in the same dialog		
CSeq				RFC 3261 [15]
value	A4	must be present, value not checked		
value	A5	value of CSeq sent by the UE within its previous request in the same dialog but increased by one		
method		*INVITE*		
Supported				RFC 3261 [15] RFC6442 [98]
option-tag		*100rel*		
Geolocation locationURI	A8	cid-url indicating the Content-Id of the PIDF-LO within the multipart MIME body of INVITE request. (Note that location-by-reference URI is not allowed as the SS does not provide any external storage for location info for the UE to refer.)	Rel-9	RFC6442 [98]
Geolocation-Routing	A8	'yes'	Rel-9	RFC 6442 [98]
Require		(header optional in A2 and not present in A6)		RFC 3261 [15] RFC 3312 [31] RFC 3329 [21]
option-tag	A1, A7	*sec-agree*		
Proxy-Require		(header optional in A2 and not present in A6)		RFC 3261 [15] RFC 3329 [21]
option-tag	A1, A7	*sec-agree*		
Security-Verify	A1, A7	(not present in A2 or A6)		RFC 3329 [21]
sec-mechanism		same value as SecurityServer header sent by SS		
Contact				RFC 3261 [15] RFC 3840 [63] RFC 5627 [61] RFC 5626 [109]
addr-spec	A1, A7	SIP URI with IP address or FQDN and protected server port of UE or GRUU as returned by the SS in registration		
	A2	SIP URI with IP address or FQDN and unprotected server port of UE or GRUU as returned by the SS in registration		
	A6	SIP URI with IP address and unprotected server port of UE		
feature-param	A6	*+sip.instance="<urn:gsma:imei*: (gsma-specifier-defined-substring)' where gsma-specifier-defined-substring shall be the IMEI code of the UE, coded as specified in draft-montemurro-gsma-imei-urn, without optional parameters		
	A3	*+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"* (see NOTE 2)		
feature-param	A10	*video*		
feature-param	A12	*g.3gpp.srvcc-alerting*		
Content-Type				RFC 3261 [15]

Header/param	Cond	Value/remark	Rel	Reference
media-type		*application/sdp or multipart/mixed (when A8)*		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
P-Access-Network-Info		(header optional when A2)		RFC 3455 [18]
access-net-spec		access network technology and, if applicable, the cell ID		
Accept		(header optional when A5)	Rel-7	RFC 3261 [15]
Media-range	A4	*application/sdp,application/3gpp-ims+xml* (additional medias can be added in any order)		
P-Preferred-Service				RFC 6050 [68]
Service-ID	A3	*urn:urn-7:3gpp-service.ims.icsi.mmtel*		
P-Preferred-Identity				RFC 3325 [89]
PPreferredID-value	A7	px_EmergencyPublicUserIdentity		
Accept-Contact				RFC 3841 [64]
ac-value	A3	*+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"* (see NOTE 2)		
ac-value	A11	*video*		
Content-Length				RFC 3261 [15]
Value		length of message-body		
Message-body		The message body shall contain the following elements: a) SDP offer, contents as specified within the specific test cases referring to this common message. If condition A8 applies the SDP shall be one element within the multipart-MIME encapsulation; b) if condition A8 applies, the multipart-mime body shall also contain a PIDF-LO element mapped to the same Content-ID which can be found from the Geolocation header The PIDF-LO shall contain at least the following elements: - One or more 'geopriv' elements, each containing: - One 'location-info' element describing the location of the UE; and - One 'usage-rules' element describing the limitations of the usage of the location info.		RFC 4119 [99]

Condition	Explanation
A1	IMS security (A.6a/2 3GPP TS 34.229-2 [5])
A2	GIBA (A.6a/1 3GPP TS 34.229-2 [5])
A3	UE supports MTSI (A.3A/50 3GPP TS 34.229-2 [5])
A4	INVITE creating a dialog
A5	re-INVITE within a dialog
A6	INVITE for creating an emergency session in case of no registration
A7	INVITE for creating an emergency session within an emergency registration
A8	UE uses Geolocation header to provide its geographical location for emergency session setup, has obtained its location and is setting up an emergency session
A9	UE supports Session-ID (A.12/30 3GPP TS 34.229-2 [5])
A10	UE indicates video media feature tag in REGISTER and INVITE request (A.12/32 3GPP TS 34.229-2 [5])
A11	INVITE for creating a video call and UE supports video media feature tag (A.12/32 3GPP TS 34.229-2 [5])
A12	INVITE for creating a voice call and UE supports g.3gpp.srvcc-alerting media feature tag (A.12/34 3GPP TS 34.229-2 [5])

NOTE 1: All choices for applicable conditions are described for each header.

NOTE 2: The '=' may include optional linear white spaces according to the EQUAL definition in chapter 25.1, RFC 3261 [15].

NOTE 3: According to TS 24.229 clause 5.1.1.1A and 5.1.6.2 [10] when the UE is using ISIM the emergency public user identity is the first public user identity in the list stored in the ISIM; when there is no ISIM it is the default public user id if the UE registered or the temporary user id (derived from IMSI) else.

A.2.2 100 Trying for INVITE

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*100*		
Reason-Phrase		*Trying*		
Via				RFC 3261 [15]
via-parm		same value as received in INVITE message		
From				RFC 3261 [15]
addr-spec		same value as received in INVITE message		
tag		same value as received in INVITE message		
To				RFC 3261 [15]
addr-spec		same value as received in INVITE message		
tag	A1	not present		
tag	A2	**Any value not present**		
Call-ID				RFC 3261 [15]
callid		same value as received in INVITE message		
CSeq				RFC 3261 [15]
value		same value as received in INVITE message		
Content-Length				RFC 3261 [15]
value		0		

Condition	Explanation
A1	100 Trying sent from SS
A2	100 Trying sent from UE

A.2.3 183 Session Progress for INVITE

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*183*		
Reason-Phrase		*Session Progress*		
Record-Route		order of the parameters in this header must be like in this table		RFC 3261 [15]
rec-route	A1	<sip:pcscf.other.com;*lr*>, <sip:scscf.other.com;*lr*>, <sip:orig@px_scscf;*lr*>, <sip:px_pcscf: protected server port of SS;*lr*>		
rec-route	A3	<sip:pcscf.other.com;*lr*>, <sip:scscf.other.com;*lr*>, <sip:orig@px_scscf;*lr*>, <sip:px_pcscf: unprotected server port of SS (optional);*lr*>		
rec-route	A2	same value as received in INVITE		
rec-route	A4	same value as received in INVITE		
Via				RFC 3261 [15]
via-parm		same value as received in INVITE message		
Require				RFC 3261 [15]
option-tag		*100rel*		
From				RFC 3261 [15]
addr-spec		same value as received in INVITE message		
tag		same value as received in INVITE message		
To				RFC 3261 [15]
addr-spec		same value as received in INVITE message		
tag		common to-tag (invite)		
P-Asserted-Identity	A5	px_EmergencyTelURI		RFC 3325 [89]
addr-spec		A tel URI that can be recognized as valid emergency numbers if dialled by the user are specified in 3GPP TS 22.101 [39]. The emergency numbers 112 and 911 are stored on the ME, in accordance with 3GPP TS 22.101 [39]		
uri-parameter		*lr*		
Contact				RFC 3261 [15]
addr-spec	A1, A3	px_CalleeContactUri		
addr-spec	A2	SIP URI with IP address or FQDN and protected server port of UE		
addr-spec	A4	SIP URI with IP address or FQDN and unprotected server port of UE		
feature-param		*+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"*(see NOTE 2)		
feature-param	A6, A7	*video*		
Rseq				RFC 3262 [33]
response-num		arbitrary value		
Call-ID				RFC 3261 [15]
callid		same value as received in INVITE message		
Session-ID				draft-kaplan-dispatch-session-id [115]
sess-id		same value as received in INVITE message, if Session-ID header field exists in received INVITE message, otherwise, not present.		
CSeq				RFC 3261 [15]
value		same value as received in INVITE message		
Content-Type				RFC 3261 [15]
media-type		*application/sdp*		
Content-Length				RFC 3261 [15]
value		length of message-body		

Condition	Explanation
A1	183 sent by the SS (IMS security ,A.6a/2 3GPP TS 34.229-2 [5])
A2	183 sent by the UE (IMS security ,A.6a/2 3GPP TS 34.229-2 [5])
A3	183 sent by the SS (GIBA, A.6a/1 3GPP TS 34.229-2 [5])
A4	183 sent by the UE (GIBA, A.6a/1 3GPP TS 34.229-2 [5])

A5	183 sent by the SS for INVITE for creating an emergency session
A6	183 sent by SS for a video call and UE supports video media feature tag (A.12/32 3GPP TS 34.229-2 [5])
A7	183 sent by UE for a video call and UE supports video media feature tag (A.12/32 3GPP TS 34.229-2 [5])

NOTE1: All choices for applicable conditions are described for each header.

NOTE 2: The '=' may include optional linear white spaces according to the EQUAL definition in chapter 25.1, RFC 3261 [15].

A.2.4 PRACK

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*PRACK*		
Request-URI		same URI value as the recipient of PRACK has earlier sent in its Contact header within the same dialog		
SIP-Version		*SIP/2.0*		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP)		
sent-by		*same value as in INVITE message*		
via-branch		value starting with "*z9hG4bK"*		
Route		(header missing when A3 or A4)		RFC 3261 [15]
route-param	A1, A2	URIs of the Record-Route header of 183 response (or 180 when applicable) in reverse order		
From				RFC 3261 [15]
addr-spec		SIP URI of the UE when PRACK is sent by the UE, but SIP URI of the SS when PRACK is sent by the SS. URI must be the same as used for the endpoint in the earlier requests within the dialog.		
tag		tag value corresponding to the SIP URI in the From header		
To				RFC 3261 [15]
addr-spec		SIP URI of the SS when PRACK is sent by the UE, but SIP URI of the UE when PRACK is sent by the SS. URI must be the same as used for the endpoint in the earlier requests within the dialog.		
tag		tag value corresponding to the SIP URI in the To header		
Call-ID				RFC 3261 [15]
callid		same value as received in INVITE message		
Session-ID				draft-kaplan-dispatch-session-id [115]
sess-id		same value as received in INVITE message, if Session-ID header field exists in received INVITE message, otherwise, not present.		
CSeq				RFC 3261 [15]
value		value of CSeq sent by the endpoint within its previous request in the same dialog but increased by one		
method		*PRACK*		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
RAck				RFC 3262 [33]
response-num		same value as in RSeq header of the reliable response		
cseq-num		same value as in CSeq of reliable response		
method		same value as in CSeq of reliable response		
P-Access-Network-Info	A1	(header optional when A2) , header missing when A3 or A4		RFC 3455 [18]
access-net-spec		access network technology and, if applicable, the cell ID		
Content-Type		header shall be present only if there is SDP in message-body		RFC 3261 [15]
media-type		*application/sdp*		
Content-Length				RFC 3261 [15]
value		length of message-body		
Message-body		Optional SDP body. If included then the contents of the SDP shall be checked as described in the Test requirements section of the test case.		RFC 4566 [27] RFC 3264 [30] RFC 3312 [31]

Condition	Explanation
A1	PRACK sent by the UE (IMS security ,A.6a/2 3GPP TS 34.229-2 [5])
A2	PRACK sent by the UE (GIBA, A.6a/1 3GPP TS 34.229-2 [5])
A3	PRACK sent by the SS (IMS security ,A.6a/2 3GPP TS 34.229-2 [5])
A4	PRACK sent by the SS (GIBA, A.6a/1 3GPP TS 34.229-2 [5])

A.2.5 UPDATE

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*UPDATE*		
Request-URI		same URI value as the recipient of UPDATE has earlier sent in its Contact header within the same dialog		
SIP-Version		*SIP/2.0*		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP)		
sent-by		*same value as in INVITE message*		
via-branch		value starting with "*z9hG4bK"*		
Route		(header missing when A3 or A4)		RFC 3261 [15]
route-param	A1, A2	URIs of the Record-Route header of 183 response in reverse order		
From				RFC 3261 [15]
addr-spec		SIP URI of the UE when UPDATE is sent by the UE, but SIP URI of the SS when UPDATE is sent by the SS. URI must be the same as used for the endpoint in the earlier requests within the dialog.		
tag		tag value corresponding to the SIP URI in the From header		
To				RFC 3261 [15]
addr-spec		SIP URI of the SS when UPDATE is sent by the UE, but SIP URI of the UE when UPDATE is sent by the SS. URI must be the same as used for the endpoint in the earlier requests within the dialog.		
tag		tag value corresponding to the SIP URI in the To header		
Call-ID				RFC 3261 [15]
callid		same value as received in INVITE message		
Session-ID				draft-kaplan-dispatch-session-id [115]
sess-id		same value as received in INVITE message, if Session-ID header field exists in received INVITE message, otherwise, not present.		
CSeq				RFC 3261 [15]
value		value of CSeq sent by the endpoint within its previous request in the same dialog but increased by one		
method		*UPDATE*		
Require		(header optional in A2) , header missing when A3 or A4		RFC 3261 [15] RFC 3329 [21]
option-tag	A1	*sec-agree*		
Proxy-Require		(header optional in A2) , header missing when A3 or A4		RFC 3261 [15] RFC 3329 [21]
option-tag	A1	*Sec-agree*		
Max-Forwards				RFC 3261 [15]
value		Non-zero value		
Security-Verify	A1	(header missing when A2, A3 or A4)		RFC 3329 [21]
sec-mechanism		same value as SecurityServer header sent by SS		
P-Access-Network-Info	A1	(header optional when A2) (header missing when A2, A3 or A4)		RFC 3455 [18]
access-net-spec		access network technology and, if applicable, the cell ID		
Content-Type				RFC 3261 [15]
media-type		*application/sdp*		
Content-Length				RFC 3261 [15]
value		length of message-body		
Message-body		Contents of the SDP body shall be checked as described in the Test requirements section of the test case.		RFC 4566 [27] RFC 3264 [30] RFC 3312 [31]

Condition	Explanation
A1	UPDATE sent by the UE (IMS security ,A.6a/2 3GPP TS 34.229-2 [5])
A2	UPDATE sent by the UE (GIBA, A.6a/1 3GPP TS 34.229-2 [5])
A3	UPDATE sent by the SS (IMS security ,A.6a/2 3GPP TS 34.229-2 [5])
A4	UPDATE sent by the SS (GIBA, A.6a/1 3GPP TS 34.229-2 [5])

NOTE1: All choices for applicable conditions are described for each header.

A.2.6 180 Ringing for INVITE

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*180*		
Reason-Phrase		*Ringing*		
Record-Route				RFC 3261 [15]
rec-route	A7	as defined for the common 183 response, see A.2.3 <*sip:orig*@px_ecscf*;lr*>, <*sip:*px_pcscf:unprotected server port of SS*;lr*>		
Via				RFC 3261 [15]
via-parm		same value as received in INVITE message		
Require				RFC 3261 [15]
option-tag	A3	*100rel*		
From				RFC 3261 [15]
addr-spec		same value as received in INVITE message		
tag		same value as received in INVITE message		
To				RFC 3261 [15]
addr-spec		same value as received in INVITE message		
tag		as defined for the common 183 response, see A.2.3		
P-Asserted-Identity	A4	px_EmergencyTelURI		RFC 3325 [89]
addr-spec		A tel URI that can be recognized as valid emergency numbers if dialled by the user are specified in 3GPP TS 22.101 [39]. The emergency numbers 112 and 911 are stored on the ME, in accordance with 3GPP TS 22.101 [39]		
uri-parameter		*lr*		
Contact				RFC 3261 [15]
addr-spec		as defined for the common 183 response, see A.2.3		
feature-param	A5	*g.3gpp.srvcc-alerting*		
Rseq				RFC 3262 [33]
response-num	A3	previous RSeq number sent in the same direction incremented by one		
Call-ID				RFC 3261 [15]
callid		same value as received in INVITE message		
Session-ID				draft-kaplan-dispatch-session-id [115]
sess-id		same value as received in INVITE message, if Session-ID header field exists in received INVITE message, otherwise, not present.		
CSeq				RFC 3261 [15]
value		same value as received in INVITE message		
P-Access-Network-Info		(header missing when A1)		
access-net-spec	A2	access network technology and, if applicable, the cell ID		
Feature-Caps				
feature-param	A6	*g.3gpp.srvcc-alerting*		
Content-Length				RFC 3261 [15]
value		length of message-body		

Condition	Explanation
A1	180 sent by the SS
A2	180 sent by the UE
A3	Response sent reliably (e.g. always when it contains an SDP body)

A4	180 sent by the SS when setting up an emergency call
A5	180 sent by the UE for a voice call and UE supports g.3gpp.srvcc-alerting media feature tag (A.12/34 3GPP TS 34.229-2 [5])
A6	180 sent by the SS for a voice call and UE supports g.3gpp.srvcc-alerting media feature tag (A.12/34 3GPP TS 34.229-2 [5])
A7	Response sent by SS for emergency call without emergency registration

A.2.7 ACK

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*ACK*		
Request-URI		*same value as in PRACK message*		
SIP-Version		*SIP/2.0*		
Via				RFC 3261 [15]
sent-protocol	A1	*SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP)		
	A2	*same as in INVITE*		
sent-by		*same value as in INVITE message*		
via-branch	A3	value starting with *"z9hG4bk"*		
via-branch	A4	Same value as received in INVITE		
Route		(header missing when A2)		RFC 3261 [15]
route-param	A1	URIs of the Record-Route header of 183, 180 or 200 response (whichever response used for INVITE to be acknowledged and contained Record-Route header) in reverse order		
From				RFC 3261 [15]
addr-spec		SIP URI of the UE when ACK is sent by the UE, but SIP URI of the SS when ACK is sent by the SS. URI must be the same as used for the endpoint in the earlier requests within the dialog.		
tag		tag value corresponding to the dialog for which ACK is sent (same as from-tag in the INVITE message)		
To				RFC 3261 [15]
addr-spec		SIP URI of the SS when ACK is sent by the UE, but SIP URI of the UE when ACK is sent by the SS. URI must be the same as used for the endpoint in the earlier requests within the dialog.		
tag		tag value corresponding to the dialog for which ACK is sent (as chosen in an earlier response of the dialog)		
Call-ID				RFC 3261 [15]
callid		same value as received in INVITE message		
CSeq				RFC 3261 [15]
value		same value as received in INVITE message		
method		*ACK*		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
P-Access-Network-Info		must **not** be present		RFC 3455 [18]
Session-ID				draft-kaplan-dispatch-session-id [115]
sess-id		same value as received in INVITE message, if Session-ID header field exists in received INVITE message, otherwise, not present.		
Content-Length				RFC 3261 [15]
value		0		

Condition	Explanation
A1	ACK sent by the UE

A2	ACK sent by the SS
A3	ACK for 2xx response
A4	ACK for non-2xx response

A.2.8 BYE

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*BYE*		
Request-URI		same URI value as the recipient of BYE has earlier sent in its Contact header within the same dialog		
SIP-Version		*SIP/2.0*		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP)		
sent-by	A1, A2	MO Call has been established: *same value as in INVITE message* MT Call has been established: same value as defined in A.2.1 (IP address or FQDN)		
	A3, A4	same values as defined in A.2.9 (There is more than one value)		
via-branch		value starting with "*z9hG4bK"*		
Route		(header missing when A3 or A4)		RFC 3261 [15]
route-param	A1, A2	MO Call has been established: URIs of the Record-Route header of 183 response in reverse order (or any other response creating the dialog according. to RFC 3261 clause 12.1 [15]) MT Call has been established: same value as defined in A.2.9		
From				RFC 3261 [15]
addr-spec		SIP URI of the UE when BYE is sent by the UE, but SIP URI of the SS when BYE is sent by the SS. URI must be the same as used for the endpoint in the earlier requests within the dialog.		
tag		tag value corresponding to the SIP URI in the From header		
To				RFC 3261 [15]
addr-spec		SIP URI of the SS when BYE is sent by the UE, but SIP URI of the UE when BYE is sent by the SS. URI must be the same as used for the endpoint in the earlier requests within the dialog.		
tag		tag value corresponding to the SIP URI in the To header		
Call-ID				RFC 3261 [15]
callid		same value as received in INVITE message		
Session-ID				draft-kaplan-dispatch-session-id [115]
sess-id		same value as received in INVITE message, if Session-ID header field exists in received INVITE message, otherwise, not present.		
CSeq				RFC 3261 [15]
value		value of CSeq sent by the UE within its previous request in the same dialog but increased by one		
method		*BYE*		
Require		(header optional in A2), header missing when A3 or A4		RFC 3261 [15] RFC 3329 [21]
option-tag	A1	*sec-agree*		
Proxy-Require		(header optional in A2), header missing when A3 or A4		RFC 3261 [15] RFC 3329 [21]
option-tag	A1	*sec-agree*		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
Security-Verify	A1	(header missing when A2, A3 or A4)		RFC 3329 [21]
sec-mechanism		same value as SecurityServer header sent by SS		
P-Access-Network-Info	A1	(header optional in A2) , header missing when A3 or A4		RFC 3455 [18]
access-net-spec		access network technology and, if applicable, the cell ID		
Content-Length				RFC 3261 [15]
value		length of message body		

Condition	Explanation
A1	BYE sent by the UE (IMS security ,A.6a/2 3GPP TS 34.229-2 [5])

A2	BYE sent by the UE (GIBA, A.6a/1 3GPP TS 34.229-2 [5])
A3	BYE sent by the SS (IMS security ,A.6a/2 3GPP TS 34.229-2 [5])
A4	BYE sent by the SS (GIBA, A.6a/1 3GPP TS 34.229-2 [5])

NOTE1: All choices for applicable conditions are described for each header.

A.2.9 INVITE for MT Call

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261[15]
Method		*INVITE*		
Request-URI	A4	UE"s registered contact address in SIP URI form, as provided in the Contact header of the REGISTER message		
Request-URI	A5	UE"s contact address in SIP URI form, as provided in the Contact header within any response or request within the dialog		
SIP-Version		*SIP/2.0*		
Via				RFC 3261[15]
sent-protocol		*SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP)		
sent-by	A1	The SS P-CSCF address and the SS protected server port		
sent-by	A2	The SS P-CSCF address and the SS unprotected server port (optional)		
via-branch		Value starting with "*z9hG4bK"*		
Via		In addition to the via-parm entry for the SS, the following via-parm entries are included:		RFC 3261[15]
via-parm		*SIP/2.0/UDP scscf1.3gpp.org;branch=z9hG4bK1234567890, SIP/2.0/UDP scscf2.3gpp.org;branch=z9hG4bK2345678901, SIP/2.0/UDP pcscf2.3gpp.org;branch=z9hG4bK3456789012, SIP/2.0/UDP caller.3gpp.org:6543;branch=z9hG4bK4567890123* Note that the branch values shown above are examples only. All of them must start with the magic cookie *z9hG4bK* but SS can build the rest of the string in a random way.		
Record-Route				RFC 3261[15]
rec-route	A1	<sip: SS P-CSCF address: protected server port of SS ;lr>		
rec-route	A2	<sip: SS P-CSCF address SS unprotected server port (optional);lr>		
Record-Route		In addition to the rec-route entry for the SS, the following rec-route entries are included:		RFC 3261[15]
rec-route		*<sip:term@scscf1.3gpp.org;lr>, <sip:orig@scscf2.3gpp.org;lr>, <sip:pcscf2.3gpp.org;lr>*		
From				RFC 3261[15]
addr-spec	A4	SIP URI of the SS representing the calling UE		
tag	A4	any value (e.g. abc1)		
addr-spec	A5	SIP URI of the SS representing the calling UE as used in any previous request in the same dialog (In the earlier requests within the same dialog this URI appears in To header within requests sent by the UE and in From header within requests sent by the SS)		
tag	A5	tag value corresponding to the SIP URI of the SS in the same dialog. (In the earlier requests within the same dialog this tag appears in To header within requests sent by the UE and in From header within requests sent by the SS)		
To				RFC 3261[15]
addr-spec	A4	SIP URI of the UE"s default public user id		
tag	A4	not present		
addr-spec	A5	SIP URI of the UE as used in any previous request in the same dialog (In the earlier requests within the same dialog this URI appears in From header within requests sent by the UE and in To header within requests sent by the SS)		
tag	A5	tag value corresponding to the SIP URI of the UE in the same dialog. (In the earlier requests within the same dialog this tag appears in From header within requests sent by the UE and in To header within requests sent by the SS)		
Call-ID				RFC 3261[15]
callid	A4	a random text string generated by the SS		

Header/param	Cond	Value/remark	Rel	Reference
callid	A5	value of Call-ID as in any previous request in the same dialog		
Session-ID		(header exists when A6)		draft-kaplan-dispatch-session-id [115]
sess-id	A4	text string generated by the SS, SHA-1 hashing the Call-ID header value		
sess-id	A5	value of Session-ID as in any previous request in the same dialog		
CSeq				RFC 3261[15]
value	A4	any value (e.g. 4711)		
value	A5	value of CSeq sent by the SS within its previous request in the same dialog but increased by one		
method		*INVITE*		
Supported				RFC 3261[15]
option-tag		*100rel*		
P-Called-Party-ID		One of the UE"s registered, non-barred public ID		RFC 3455[18]
Contact				RFC 3261[15]
addr-spec	A1	SIP URI with IP address or FQDN and protected server port of the calling UE, for example 'sip:caller@3gpp.org:6543'		
addr-spec	A2	SIP URI with IP address or FQDN and unprotected server port of the calling UE		
feature-param	A3	*+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"*		
feature-param	A7	*video*		
Content-Type				RFC 3261[15]
media-type		*application/sdp*		
Max-Forwards				RFC 3261[15]
value		non-zero value		
Accept			Rel-7	RFC 3261 [15
media-range	A4	*application/sdp, application/3gpp-ims+xml*		
P-Asserted-Service				RFC 6050 [68]
Service-ID	A3	*urn:urn-7:3gpp-service.ims.icsi.mmtel*		
Accept-Contact				RFC 3841 [64]
ac-value	A3	**;+g.3gpp.icsi-ref="urn%3Aurn-7%3A3gpp-service.ims.icsi.mmtel"*		
ac-value	A8	*video*		
Content-Length				RFC 3261[15]
value		length of message-body		
Feature-Caps				
feature-param	A9	*g.3gpp.srvcc-alerting*		

Condition	Explanation
A1	IMS security (A.6a/2 3GPP TS 34.229-2 [5])
A2	GIBA (A.6a/1 3GPP TS 34.229-2 [5])
A3	UE supports MTSI (A.3A/50 3GPP TS 34.229-2 [5])
A4	INVITE creating a dialog
A5	re-INVITE within a dialog
A6	UE supports Session-ID (A.12/30 3GPP TS 34.229-2 [5])
A7	UE indicates video media feature tag in REGISTER and INVITE request (A.12/32 3GPP TS 34.229-2 [5])
A8	INVITE for creating a video call and UE supports video media feature tag (A.12/32 3GPP TS 34.229-2 [5])
A9	INVITE for creating a voice call and UE supports g.3gpp.srvcc-alerting media feature tag (A.12/34 3GPP TS 34.229-2 [5])

NOTE1: All choices for applicable conditions are described for each header.

A.2.10 MO REFER

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*REFER*		
Request-URI		same URI value as the SS has earlier sent in its Contact header within the same dialog		
SIP-Version		*SIP/2.0*		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP)		
sent-by	A1	IP address or FQDN and protected server port of the UE		
	A2	IP address or FQDN and unprotected server port of the UE		
via-branch		value starting with "*z9hG4bK*"		
Route		order of the parameters in this header must be like in this table		RFC 3261 [15]
route-param	A1	<*sip:*px_pcscf: protected server port of SS *;lr*>, <*sip:*px_scscf*;lr*>		
	A2	<*sip:*px_pcscf: unprotected server port of SS (optional)*;lr*>, <*sip:*px_scscf*;lr*		
From				RFC 3261 [15]
addr-spec		local SIP URI of the UE which must be the same URI as used for the UE in the earlier requests within the dialog		
tag		tag value corresponding to the SIP URI in the From header		
To				RFC 3261 [15]
addr-spec		remote SIP URI of the SS which must be the same URI as used for SS in the earlier requests within the dialog.		
tag		tag value corresponding to the SIP URI in the To header		
Call-ID				RFC 3261 [15]
callid		same value as in the first INVITE during the call setup		
Session-ID				draft-kaplan-dispatch-session-id [115]
sess-id		same value as received in INVITE message, if Session-ID header field exists in received INVITE message, otherwise, not present.		
CSeq				RFC 3261 [15]
value		value of CSeq sent by the UE within its previous request in the same dialog but increased by one		
method		*REFER*		
Require		(header optional in A2)		RFC 3261 [15] RFC 3312 [31] RFC 3329 [21]
option-tag	A1	*sec-agree*		
Proxy-Require		(header optional in A2)		RFC 3261 [15] RFC 3329 [21]
option-tag	A1	*sec-agree*		
Security-Verify	A1	(not present in A2)		RFC 3329 [21]
sec-mechanism		same value as SecurityServer header sent by SS		
Contact				RFC 3261 [15]
addr-spec	A1	SIP URI with IP address or FQDN and protected server port of UE or GRUU as returned by the SS in registration		
	A2	SIP URI with IP address or FQDN and unprotected server port of UE or GRUU as returned by the SS in registration		
Refer-To				RFC 3515 [72]
addr-spec		SIP or Tel URI of the transfer target		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
P-Access-Network-Info	A1	(header optional when A2)		RFC 3455 [18]

Header/param	Cond	Value/remark	Rel	Reference
access-net-spec		access network technology and, if applicable, the cell ID		
Content-Length				RFC 3261 [15]
Value		length of message-body		

Condition	Explanation
A1	IMS security (A.6a/2 3GPP TS 34.229-2 [5])
A2	GIBA (A.6a/1 3GPP TS 34.229-2 [5])

A.2.11 MT NOTIFY for refer package

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*NOTIFY*		
Request-URI		same URI value which the UE sent in its Contact header within the REFER request		
SIP-Version		*SIP/2.0*		
Via		order of the parameters in this header must be like in this table		RFC 3261 [15]
via-parm1:				
Sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by	A1	IP address and protected server port of SS		
sent-by	A2	IP address and unprotected server port of SS (optional)		
via-branch		value starting with "*z9hG4bK"*		
via-parm2:		In addition to the via-parm entry for the SS, the following via-parm entries are included:		
via-parm		*SIP/2.0/UDP scscf1.3gpp.org;branch=z9hG4bK1234567890, SIP/2.0/UDP scscf2.3gpp.org;branch=z9hG4bK2345678901, SIP/2.0/UDP pcscf2.3gpp.org;branch=z9hG4bK3456789012, SIP/2.0/UDP uas.3gpp.org:6543;branch=z9hG4bK4567890123* Note that the branch values shown above are examples only. All of them must start with the magic cookie *z9hG4bK* but SS can build the rest of the string in a random way.		
From				RFC 3261 [15]
addr-spec		SIP URI of the SS which must be the same URI as used for the SS in the earlier requests within the dialog		
tag		tag value corresponding to the SIP URI in the From header		
To				RFC 3261 [15]
addr-spec		SIP URI of the UE which must be the same as used for the UE in the earlier requests within the dialog.		
tag		tag value corresponding to the SIP URI in the To header		
Call-ID				RFC 3261 [15]
callid		same value as in the INVITE (and REFER) message		
Session-ID				draft-kaplan-dispatch-session-id [115]
sess-id		same value as received in INVITE (and REFER) message, if Session-ID header field exists in received INVITE (and REFER) message, otherwise, not present.		
CSeq	A1,A2			RFC 3261 [15]
value		value of CSeq sent by the SS within its previous request in the same dialog but increased by one		
method		*NOTIFY*		
Contact				RFC 3261 [15]
addr-spec	A1	SIP URI with IP address or FQDN and protected server port of the SS (transferee)		
addr-spec	A2	SIP URI with IP address or FQDN and unprotected server port of the SS (transferee)		
Content-Type				RFC 3261 [15] RFC 3680 [22]
media-type		*message/sipfrag*		
Event	A1,A2			RFC 3265 [34] RFC 3515 [72]
event-type		*refer*		
Max-Forwards				RFC 3261 [15]
value		*69*		

Header/param	Cond	Value/remark	Rel	Reference
Subscription-State				RFC 3265[34]
substate-value		*active*		
expires		*300*		
Content-Length				RFC 3261 [15] RFC 3680 [22]
value		length of message-body		

Condition	Explanation
A1	IMS security (A.6a/2 3GPP TS 34.229-2 [5])
A2	GIBA (A.6a/1 3GPP TS 34.229-2 [5])

A.2.12 MT REFER

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*REFER*		
Request-URI		same URI value as that which the UE has earlier sent in its Contact header within the dialog created by the INVITE sent by the UE when initiating the call to be transferred		
SIP-Version		*SIP/2.0*		
Via		order of the parameters in this header must be like in this table		RFC 3261 [15]
via-parm1:				
Sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by	A1	IP address and protected server port of SS		
sent-by	A2	IP address and unprotected server port of SS (optional)		
via-branch		value starting with "*z9hG4bK"*		
via-parm2:		In addition to the via-parm entry for the SS, the following via-parm entries are included:		
via-parm		*SIP/2.0/UDP scscf1.3gpp.org;branch=z9hG4bK1234567890, SIP/2.0/UDP scscf2.3gpp.org;branch=z9hG4bK2345678901, SIP/2.0/UDP pcscf2.3gpp.org;branch=z9hG4bK3456789012, SIP/2.0/UDP uas.3gpp.org:6543;branch=z9hG4bK4567890123* Note that the branch values shown above are examples only. All of them must start with the magic cookie *z9hG4bK* but SS can build the rest of the string in a random way.		
From				RFC 3261 [15]
addr-spec		SIP URI of the SS which must be the same URI as used for the SS in the earlier requests within the dialog created by the INVITE sent by the UE when initiating the call to be transferred		
tag		tag value corresponding to the SIP URI in the From header		
To				RFC 3261 [15]
addr-spec		SIP URI of the UE which must be the same URI as used for UE in the earlier requests within the dialog created by the INVITE sent by the UE when initiating the call to be transferred		
tag		tag value corresponding to the SIP URI in the To header		
Call-ID				RFC 3261 [15]
callid		same value as in the first INVITE sent by the UE during setup of the call to be transferred		
Session-ID				draft-kaplan-dispatch-session-id [115]
sess-id		same value as in the first INVITE sent by the UE during setup of the call to be transferred, if Session-ID header field exists in the first INVITE sent by the UE during setup of the call to be transferred, otherwise, not present.		
CSeq				RFC 3261 [15]
value		value of CSeq sent by the SS within its previous request in the dialog created by the INVITE sent by the UE when initiating the call to be transferred, but increased by one		
method		*REFER*		
Contact				RFC 3261 [15]
addr-spec	A1	SIP URI with IP address or FQDN and protected server port of the SS (transferor)		

Header/param	Cond	Value/remark	Rel	Reference
	A2	SIP URI with IP address or FQDN and unprotected server port of the SS (transferor)		
Refer-To				RFC 3515 [72]
addr-spec		SIP or Tel URI of the transfer target		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
P-Access-Network-Info	A1	(header optional when A2)		RFC 3455 [18]
access-net-spec		access network technology and, if applicable, the cell ID		
Content-Length				RFC 3261 [15]
Value		length of message-body		

Condition	Explanation
A1	IMS security (A.6a/2 TS 34.229-2 [5])
A2	GIBA (A.6a/1 TS 34.229-2 [5])

A.2.13 MO NOTIFY for refer package

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*NOTIFY*		
Request-URI		same URI value which the SS sent in its Contact header within the REFER request		
SIP-Version		*SIP/2.0*		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by	A1	IP address or FQDN and protected server port of the UE		
	A2	IP address or FQDN and unprotected server port of UE		
via-branch		value starting with "*z9hG4bK"*		
Route		order of the parameters in this header must be like in this table		RFC 3261 [15]
route-param	A1	<*sip:*px_pcscf: protected server port of SS *;lr*>, <*sip:*px_scscf;*lr*>		
	A2	<*sip:*px_pcscf: unprotected server port of SS (optional)*;lr*>, <*sip:*px_scscf;*lr*		

Header/param	Cond	Value/remark	Rel	Reference
From				RFC 3261 [15]
addr-spec		Local SIP URI of the UE which must be the same URI as used for the UE in the earlier requests within the dialog created by the INVITE sent by the UE when initiating the call to be transferred		
tag		tag value corresponding to the SIP URI in the From header		
To				RFC 3261 [15]
addr-spec		Remote SIP URI of the SS which must be the same as used for the SS in the earlier requests within the dialog created by the INVITE sent by the UE when initiating the call to be transferred.		
tag		tag value corresponding to the SIP URI in the To header		
Call-ID				RFC 3261 [15]
callid		same value as in the INVITE (and REFER) message		
Session-ID				draft-kaplan-dispatch-session-id [115]
sess-id		same value as received in INVITE (and REFER) message, if Session-ID header field exists in received INVITE (and REFER) message, otherwise, not present.		
CSeq	A1,A2			RFC 3261 [15]
value		value of CSeq sent by the SS within its previous request in the dialog created by the INVITE sent by the UE when initiating the call to be transferred, but increased by one		
method		*NOTIFY*		
Contact				RFC 3261 [15]
addr-spec	A1	SIP URI with IP address or FQDN and protected server port of the UE or GRUU as returned by the SS in registration		
addr-spec	A2	SIP URI with IP address or FQDN and unprotected server port of UE or GRUU as returned by the SS in registration		
Content-Type				RFC 3261 [15] RFC 3680 [22]
media-type		*message/sipfrag*		
Event	A1,A2			RFC 3265 [34] RFC 3515 [72]
event-type		*refer*		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
Subscription-State				RFC 3265[34]
substate-value		*active*		
expires		non-zero value		
Content-Length				RFC 3261 [15] RFC 3680 [22]
value		length of message-body		

Condition	Explanation
A1	IMS security (A.6a/2 TS 34.229-2 [5])
A2	GIBA (A.6a/1 TS 34.229-2 [5])

A.2.14 181 Call is being forwarded

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 3261 [15]
SIP-Version	*SIP/2.0*		
Status-Code	*181*		
Reason-Phrase	*Call is being forwarded*		
Via			RFC 3261 [15]
via-parm	same value as received in INVITE message		
From			RFC 3261 [15]
addr-spec	same value as received in INVITE message		
tag	same value as received in INVITE message		
To			RFC 3261 [15]
addr-spec	same value as received in INVITE message		
tag	common to-tag (invite)		
History-Info			RFC 4244 [83]
hi-targeted-to-uri	<*sip:user@company.com*>		
hi-index	*1*		
Call-ID			RFC 3261 [15]
callid	same value as received in INVITE message		
Session-ID			draft-kaplan-dispatch-session-id [115]
sess-id	same value as received in INVITE message, if Session-ID header field exists in received INVITE message, otherwise, not present.		
CSeq			RFC 3261 [15]
value	same value as received in INVITE message		
Content-Length			RFC 3261 [15]
value	0		

A.2.15 CANCEL

Header/param	Value/remark	Rel	Reference
Request-Line			RFC 3261 [15]
Method	*CANCEL*		
Request-URI	same value as in the INVITE being cancelled		
SIP-Version	*SIP/2.0*		
Via			RFC 3261 [15]
via-parm	same value as in the INVITE being cancelled		
From			RFC 3261 [15]
addr-spec	same value as in the INVITE being cancelled		
Tag	same value as in the INVITE being cancelled		
To			RFC 3261 [15]
addr-spec	same value as in the INVITE being cancelled		
tag	same value as in the INVITE being cancelled		
Call-ID			RFC 3261 [15]
Callid	same value as in the INVITE being cancelled		
Session-ID			draft-kaplan-dispatch-session-id [115]
sess-id	same value as in the INVITE being cancelled, if Session-ID header field exists in the INVITE being cancelled, otherwise, not present.		
CSeq			RFC 3261 [15]
Numeric value	same value as received in INVITE message		
Method	*CANCEL*		
Content-Length			RFC 3261 [15]
Value	0		

A.2.16 487 Request Terminated

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 3261 [15]
SIP-Version	*SIP/2.0*		
Status-Code	*487*		
Reason-Phrase	*Request Terminated*		
Via			RFC 3261 [15]
via-parm	same value as received in INVITE message		
From			RFC 3261 [15]
addr-spec	same value as received in INVITE message		
tag	same value as received in INVITE message		
To			RFC 3261 [15]
addr-spec	same value as received in INVITE message		
tag	common to-tag (invite)		
Call-ID			RFC 3261 [15]
callid	same value as received in INVITE message		
Session-ID			draft-kaplan-dispatch-session-id [115]
sess-id	same value as received in INVITE message, if Session-ID header field exists in received INVITE message, otherwise, not present.		
CSeq			RFC 3261 [15]
value	same value as received in INVITE message		
Content-Length			RFC 3261 [15]
value	0		

A.3 Generic Common Messages

A.3.1 200 OK for other requests than REGISTER or SUBSCRIBE

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*200*		
Reason-Phrase		*OK*		
Via				RFC 3261 [15]
via-parm		same value as received in request		
Record-Route		order of the parameters in this header must be like in this table		RFC 3261 [15]
rec-route	A1	<*sip:pcscf.other.com;lr*>, <*sip:scscf.other.com;lr*>, <*sip:orig*@px_scscf;*lr*>, <*sip:*px_pcscf: protected server port of SS ;*lr*>		
rec-route	A3	<*sip:pcscf.other.com;lr*>, <*sip:scscf.other.com;lr*>, <*sip:orig*@px_scscf;*lr*>, <*sip:*px_pcscf: unprotected server port of SS (optional);*lr*>		
rec-route	A2,A4,A5	same value as received in the request (if present in the request) Note: for requests other than INVITE it is not regulated if and what the UE writes into this header in a response.		
rec-route	A7	<*sip:orig*@px_ecscf;*lr*>, <*sip:*px_pcscf:unprotected server port of SS;*lr*>		
From				RFC 3261 [15]
addr-spec		same value as received in request		
tag		same value as received in request		
To				RFC 3261 [15]
addr-spec		same value as received in request		
tag		same value as received in request or common to-tag (invite) added if missing from request		
P-Asserted-Identity	A6	px_EmergencyTelURI		RFC 3325 [89]
addr-spec		A tel URI that can be recognized as valid emergency numbers if dialled by the user are specified in 3GPP TS 22.101 [39]. The emergency numbers 112 and 911 are stored on the ME, in accordance with 3GPP TS 22.101 [39]		
uri-parameter		*lr*		
Contact				
addr-spec	A1, A3	px_CalleeContactUri		
addr-spec	A2	SIP URI with IP address or FQDN and protected server port of UE		
addr-spec	A4	SIP URI with IP address or FQDN and unprotected server port of UE		
Call-ID				RFC 3261 [15]
callid		same value as received in request		
Session-ID				draft-kaplan-dispatch-session-id [115]
sess-id		same value as received in request, if Session-ID header field exists in received request, otherwise, not present.		
CSeq				RFC 3261 [15]
value		same value as received in request		
P-Access-Network-Info	A1, A2, A3	NOTE: header optional when A4		
access-net-spec	A5	access network technology and, if applicable, the cell ID		
Content-Length				RFC 3261 [15]
value		0		

Condition	Explanation
A1	Response sent by SS for INVITE/UPDATE (IMS security ,A.6a/2 TS 34.229-2 [5]))
A2	Response sent by UE for INVITE/UPDATE (IMS security ,A.6a/2 TS 34.229-2 [5]))
A3	Response sent by SS for INVITE/UPDATE (GIBA, A.6a/1 TS 34.229-2 [5]))
A4	Response sent by UE for INVITE/UPDATE (GIBA, A.6a/1 TS 34.229-2 [5]))
A5	Any response sent by the UE within a dialog
A6	Response sent by SS for INVITE for emergency call
A7	Response sent by SS for INVITE for emergency call without emergency registration

A.3.2 403 FORBIDDEN

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 3261 [15]
SIP-Version	*SIP/2.0*		
Status-Code	*403*		
Reason-Phrase	*Forbidden*		
Via			RFC 3261 [15]
via-parm	same value as received in the previous REGISTER message		
To			RFC 3261 [15]
addr-spec	same value as received in the previous REGISTER message		
tag	common to-tag (register)		
From			RFC 3261 [15]
addr-spec	same value as received in the previous REGISTER message		
Call-ID			RFC 3261 [15]
value	same value as received in the previous REGISTER message		
Session-ID			draft-kaplan-dispatch-session-id [115]
sess-id	same value as received in the previous REGISTER message, if Session-ID header field exists in the previous REGISTER message, otherwise, not present.		
CSeq			RFC 3261 [15]
value	same value as received in the previous REGISTER message		
Content-length			RFC 3261 [15]
value	0		RFC 3261 [15]

A.3.3 202 Accepted

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 3261 [15]
SIP-Version	*SIP/2.0*		
Status-Code	*202*		
Reason-Phrase	*Accepted*		
Via			RFC 3261 [15]
via-parm	same value as received in request		
From			RFC 3261 [15]
addr-spec	same value as received in request		
tag	same value as received in request		
To			RFC 3261 [15]
addr-spec	same value as received in request		
tag	same value as received in request or common to-tag (message) added if missing from request		
Call-ID			RFC 3261 [15]
callid	same value as received in request		
Session-ID			draft-kaplan-dispatch-session-id [115]
sess-id	same value as received in request, if Session-ID header field exists in received request, otherwise, not present.		
CSeq			RFC 3261 [15]
value	same value as received in request		
Content-Length			RFC 3261 [15]
value	0		

A.4 Other Default Messages

A.4.1 380 Alternative Service

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 3261 [15]
SIP-Version	*SIP/2.0*		
Status-Code	*380*		
Reason-Phrase	Alternative Service		
Via			RFC 3261 [15]
via-parm	same value as received in request		
From			RFC 3261 [15]
addr-spec	same value as received in request		
tag	same value as received in request		
To			RFC 3261 [15]
addr-spec	same value as received in request		
tag	same value as received in request or common to-tag (invite) added		
P-Asserted-Identity			RFC 3325 [89]
addr-spec	px_pcscf		
uri-parameter	*lr*		
Call-ID			RFC 3261 [15]
callid	same value as received in request		
Session-ID			draft-kaplan-dispatch-session-id [115]
sess-id	same value as received in request, if Session-ID header field exists in received request, otherwise, not present.		
CSeq			RFC 3261 [15]
value	same value as received in request		
Content-Length			RFC 3261 [15]
value	Length of message-body		
Content-Type			RFC 3261 [15]
media-type	*application/3gpp-ims+xml*		
Message-body	*<?xml version="1.0"?>* *<ims-3gpp version="1">* *<alternative-service>* *<type>emergency</type>* *<reason/>* *</alternative-service>* *</ims-3gpp>*		

A.4.2 503 Service Unavailable

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 3261 [15]
SIP-Version	*SIP/2.0*		
Status-Code	*503*		
Reason-Phrase	Service Unavailable		
Via			RFC 3261 [15]
via-parm	same value as received in request		
From			RFC 3261 [15]
addr-spec	same value as received in request		
tag	same value as received in request		
To			RFC 3261 [15]
addr-spec	same value as received in request		
tag	any arbitrary tag value added		
Call-ID			RFC 3261 [15]
callid	same value as received in request		
Session-ID			draft-kaplan-dispatch-session-id [115]
sess-id	same value as received in request, if Session-ID header field exists in received request, otherwise, not present.		
CSeq			RFC 3261 [15]
value	same value as received in request		
Content-Length			RFC 3261 [15]
value	0		
Retry-after			RFC 3261 [15], TS 24.229 [10], 5.1.2.2
period	*60* (referred to as T in the test procedure and test requirement)		
duration	*Not present*		
comment	*Not present*		

A.4.3 PUBLISH

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3903 [60]
Method		*PUBLISH*		
Request-URI		any IMPU within the set of IMPUs on ISIM		
SIP-Version		*SIP/2.0*		
Route		order of the parameters in this header must be like in this table		RFC 3261 [15] RFC 3903 [60]
route-param	A1	<*sip:*px_pcscf:protected server port of P-CSCF;*lr*>, <*sip:*px_scscf;*lr*>		
route-param	A2	<*sip:*px_pcscf: unprotected server port of P-CSCF (optional);*lr*>, <*sip:*px_scscf;*lr*>		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by	A1	IP address or FQDN and protected server port of the UE		
sent-by	A2	IP address or FQDN, port (optional) and not checked		
via-branch		value starting with "*z9hG4bK"*		
From				RFC 3261 [15]
addr-spec		any IMPU within the set of IMPUs on ISIM		
tag		must be present, value not checked but stored for later reference		
To				RFC 3261 [15]
addr-spec		any IMPU within the set of IMPUs on ISIM		
tag		must not be present		
Expires		**Optional**		RFC 3261 [15]
delta-seconds		same as registration timer		
Security-Verify	A1			RFC 3329 [21]
sec-mechanism		same value as SecurityServer header sent by SS		
Require	A1	**Optional**		RFC 3261 [15] RFC 3329 [21]
option-tag		*Not checked*		
Proxy-Require	A1	**Optional**		RFC 3261 [15] RFC 3329 [21]
option-tag		*Not checked*		
CSeq				RFC 3261 [15]
value		must be present, value not checked		
method		*PUBLISH*		
Call-ID				RFC 3261 [15]
callid		value not checked, but stored for later reference		
Session-ID	A3			draft-kaplan-dispatch-session-id [115]
sess-id		value not checked, but stored for later reference		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
P-Access-Network-Info	A1	(header optional when A2)		RFC 3455 [18]
access-net-spec		access network technology and, if applicable, the cell ID		
Event				RFC 3265 [34] RFC 3680 [22] RFC 3903 [60]
event-type		value not checked		
SIP-If-Match		optional		RFC 3903 [60]
entry-tag				
Content-Length				RFC 3261 [15]
value		length of request body, if such is present		
Message-body		optional		

Condition	Explanation
A1	IMS security (A.6a/2 TS 34.229-2 [5]))
A2	GIBA (A.6a/1 TS 34.229-2 [5]))
A3	UE supports Session-ID (A.12/30 TS 34.229-2 [5]))

NOTE1: All choices for applicable conditions are described for each header.

A.4.4 200 OK for PUBLISH

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 3261 [15]
SIP-Version	*SIP/2.0*		
Status-Code	*200*		
Reason-Phrase	*OK*		
Via			RFC 3261 [15]
via-parm	same value as received in PUBLISH message		
To			RFC 3261 [15]
addr-spec	any IMPU within the set of IMPUs on ISIM		
tag	common to-tag (subscribe dialog)		
From			RFC 3261 [15]
addr-spec	same value as received in PUBLISH message		
tag	same value as received in PUBLISH message		
Call-ID			RFC 3261 [15]
callid	same value as received in PUBLISH message		
Session-ID			draft-kaplan-dispatch-session-id [115]
sess-id	same value as received in PUBLISH message, if Session-ID header field exists in received PUBLISH message, otherwise, not present.		
CSeq			RFC 3261 [15]
value	same value as received in PUBLISH message		
Contact			RFC 3261 [15]
addr-spec	<*sip:*px_scscf>		
Expires			RFC 3261 [15] RFC 3903 [60]
delta-seconds	600000		
SIP-ETag			RFC 3903 [60]
entry-tag	unique generated tag for every request		
Content-Length			RFC 3261 [15]
value	0		

A.4.5 302 Moved Temporarily

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 3261 [15]
SIP-Version	*SIP/2.0*		
Status-Code	*302*		
Reason-Phrase	Moved Temporarily		
Via			RFC 3261 [15]
via-parm	same value as received in request		
From			RFC 3261 [15]
addr-spec	same value as received in request		
tag	same value as received in request		
To			RFC 3261 [15]
addr-spec	same value as received in request		
tag	any arbitrary tag value added		
Call-ID			RFC 3261 [15]
callid	same value as received in request		
Session-ID			draft-kaplan-dispatch-session-id [115]
sess-id	same value as received in request, if Session-ID header field exists in received request, otherwise, not present.		
CSeq			RFC 3261 [15]
value	same value as received in request		
Content-Length			RFC 3261 [15]
value	0		
Contact			RFC 3261 [15]
addr-spec	*sip:user@company.com*		

A.4.6 504 Server Time-out

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 3261 [15]
SIP-Version	*SIP/2.0*		
Status-Code	*504*		
Reason-Phrase	Server Time-out		
Via			RFC 3261 [15]
via-parm	same value as received in request		
From			RFC 3261 [15]
addr-spec	same value as received in request		
tag	same value as received in request		
To			RFC 3261 [15]
addr-spec	same value as received in request		
tag	any arbitrary tag value added		
P-Asserted-Identity			RFC 3325 [89]
addr-spec	px_scscf		
uri-parameter	*lr*		
Call-ID			RFC 3261 [15]
callid	same value as received in request		
Session-ID			draft-kaplan-dispatch-session-id [115]
sess-id	same value as received in request, if Session-ID header field exists in received request, otherwise, not present.		
CSeq			RFC 3261 [15]
value	same value as received in request		
Content-Length			RFC 3261 [15]
value	Length of message-body		
Content-Type			RFC 3261 [15]
media-type	*application/3gpp-ims+xml*		
Message-body	*<?xml version="1.0"?>* *<ims-3gpp version="1">* *<alternative-service>* *<type>restoration</type>* *<reason/>* *<action>initial-registration</action>* *</alternative-service>* *</ims-3gpp>*		

A.5 Default messages for Conferencing

A.5.1 SUBSCRIBE for conference event package

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*SUBSCRIBE*		
Request-URI		px_FinalConferenceUri		
SIP-Version		*SIP/2.0*		
Route		order of the parameters in this header must be like in this table		RFC 3261 [15]
route-param	A1	<*sip:*px_pcscf:protected server port of P-CSCF;*lr*>, <*sip:*px_scscf;*lr*>		
route-param	A2	<*sip:*px_pcscf: unprotected server port of P-CSCF (optional);*lr*>, <*sip:*px_scscf;*lr*>		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by	A1	IP address or FQDN and protected server port of the UE		
sent-by	A2	IP address or FQDN and unprotected server port of the UE		
via-branch		value starting with "*z9hG4bK"*		
From				RFC 3261 [15]
addr-spec		any IMPU within the set of IMPUs on ISIM		
tag		must be present, value not checked but stored for later reference		
To				RFC 3261 [15]
addr-spec		px_FinalConferenceUri		
tag		not present		
Contact				RFC 3261 [15]
addr-spec	A1	SIP URI with IP address or FQDN and protected server port of UE		
addr-spec	A2	SIP URI with IP address or FQDN and unprotected server port of UE		
Expires				RFC 3261 [15]
delta-seconds		must be present but value not checked		
Security-Verify	A1			RFC 3329 [21]
sec-mechanism		same value as SecurityServer header sent by SS		
Require	A1			RFC 3261 [15] RFC 3329 [21]
option-tag		*sec-agree*		
Proxy-Require	A1			RFC 3261 [15] RFC 3329 [21]
option-tag		*sec-agree*		
CSeq				RFC 3261 [15]
value		must be present, value not checked		
method		*SUBSCRIBE*		
Call-ID				RFC 3261 [15]
callid		value not checked, but stored for later reference		
Session-ID	A3			draft-kaplan-dispatch-session-id [115]
sess-id		value not checked, but stored for later reference		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
P-Access-Network-Info	A1	(header optional when A2)		RFC 3455 [18]
access-net-spec		access network technology and, if applicable, the cell ID		

Header/param	Cond	Value/remark	Rel	Reference
Accept				RFC 3261 [15]
media-range		*application/conference-info+xml*		RFC 3680 [22]
Event				RFC 3265 [34]
event-type		*conference*		RFC 3680 [22]
Content-Length				RFC 3261 [15]
value		length of request body, if such is present		

Condition	Explanation
A1	IMS security (A.6a/2 TS 34.229-2 [5]))
A2	GIBA (A.6a/1 TS 34.229-2 [5]))
A3	UE supports Session-ID (A.12/30 TS 34.229-2 [5]))

NOTE1: All choices for applicable conditions are described for each header.

A.5.2 200 OK for SUBSCRIBE

Header/param	Cond	Value/remark	Rel	Reference
Status-Line				RFC 3261 [15]
SIP-Version		*SIP/2.0*		
Status-Code		*200*		
Reason-Phrase		*OK*		
Via				RFC 3261 [15]
via-parm		same value as received in SUBSCRIBE message		
To				RFC 3261 [15]
addr-spec		any IMPU within the set of IMPUs on ISIM		
tag		common to-tag (subscribe conference dialog)		
From				RFC 3261 [15]
addr-spec		same value as received in SUBSCRIBE message		
tag		same value as received in SUBSCRIBE message		
Call-ID				RFC 3261 [15]
callid		same value as received in SUBSCRIBE message		
Session-ID				draft-kaplan-dispatch-session-id [115]
sess-id		same value as received in SUBSCRIBE message, if Session-ID header field exists in SUBSCRIBE message, otherwise, not present.		
CSeq				RFC 3261 [15]
value		same value as received in SUBSCRIBE message		
Contact				RFC 3261 [15]
addr-spec		px_FinalConferenceUri		
Expires				RFC 3261 [15]
delta-seconds		7200		
Record-Route				RFC 3261 [15]
addr-spec	A1	px_pcscf: protected server port of SS		
addr-spec	A2	px_pcscf: unprotected server port of SS (optional)		
uri-parameter		*Lr*		
Content-Length				RFC 3261 [15]
value		0		

Condition	Explanation
A1	IMS security (A.6a/2 TS 34.229-2 [5]))
A2	GIBA (A.6a/1 TS 34.229-2 [5]))

NOTE1: All choices for applicable conditions are described for each header.

A.5.3 NOTIFY for conference event package

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*NOTIFY*		
Request-URI		UE"s contact address in SIP URI form, as provided in the Contact header within the SUBSCRIBE creating the dialog		
SIP-Version		*SIP/2.0*		
Via		order of the parameters in this header must be like in this table		RFC 3261 [15]
via-parm1:				
Sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by	A1	IP address and protected server port of SS		
sent-by	A2	IP address and unprotected server port of SS (optional)		
via-branch		value starting with "*z9hG4bK"*		
via-parm2:				
sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by		px_scscf		
via-branch		value starting with "*z9hG4bK"*		
From				RFC 3261 [15]
addr-spec		px_FinalConferenceUri		
tag		tag value corresponding to the SIP URI in the From header		
To				RFC 3261 [15]
addr-spec		any IMPU within the set of IMPUs on ISIM		
tag		tag value corresponding to the SIP URI in the To header		
Call-ID				RFC 3261 [15]
callid		same as value received in SUBSCRIBE message		
Session-ID				draft-kaplan-dispatch-session-id [115]
sess-id		same value as received in SUBSCRIBE message, if Session-ID header field exists in SUBSCRIBE message, otherwise, not present.		
CSeq	A1,A2			RFC 3261 [15]
value		value of CSeq sent by the SS within its previous request in the same dialog but increased by one		
method		*NOTIFY*		
Contact				RFC 3261 [15]
addr-spec		px_FinalConferenceUri		
Content-Type				RFC 3261 [15] RFC 4575 [86]
media-type		*application/conference-info+xml*		
Event	A1,A2			RFC 3265[34] RFC 4575 [86]
event-type		*conference*		
Max-Forwards				RFC 3261 [15]
value		*69*		
Subscription-State				RFC 3265[34]
substate-value		*active*		
expires		*7200*		
Content-Length				RFC 3261 [15] RFC 4575 [86]
value		length of message-body		
Message-body		*<?xml version="1.0" encoding="UTF-8"?>* *<conference-info* *xmlns="urn:ietf:params:xml:ns:conference-info">* *entity="***px_FinalConferenceUri***"* *state="full"* *version="0"*		

Header/param	Cond	Value/remark	Rel	Reference
		<users> *<user entity="* **any IMPU within the set of IMPUs on ISIM***">* *<endpoint entity="* **Contact URI of the UE***">* *<status>connected</status>* *<joining-method>dialed-in</joining-method>* *<media id="1">* *<type>audio</type>* *<label>34567</label>* *<src-id>***SSRC of UE's RTP packets***</src-id>* *<status>sendrecv</status>* *</media>* *</endpoint>* *</users>* *</conference-info>*		

Condition	Explanation
A1	IMS security (A.6a/2 TS 34.229-2 [5]))
A2	GIBA (A.6a/1 TS 34.229-2 [5]))

NOTE1: All choices for applicable conditions are described for each header.

A.6 Default messages for Message Waiting Indication

A.6.1 SUBSCRIBE for message-summary event package

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*SUBSCRIBE*		
Request-URI		any IMPU within the set of IMPUs on ISIM or px_MessageAccountIdentity. UE shall use px_MessageAccountIdentity when that is configured to the phone as Public service identity of the message account.		
SIP-Version		*SIP/2.0*		
Route		order of the parameters in this header must be like in this table		RFC 3261 [15]
route-param	A1	<*sip:*px_pcscf:protected server port of P-CSCF;*lr*>, <*sip:*px_scscf;*lr*>		
route-param	A2	<*sip:*px_pcscf: unprotected server port of P-CSCF (optional);*lr*>, <*sip:*px_scscf;*lr*>		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by	A1	IP address or FQDN and protected server port of the UE		
sent-by	A2	IP address or FQDN and unprotected server port of the UE		
via-branch		value starting with "*z9hG4bK"*		
From				RFC 3261 [15]
addr-spec		any IMPU within the set of IMPUs on ISIM		
tag		must be present, value not checked but stored for later reference		
To				RFC 3261 [15]
addr-spec		any IMPU within the set of IMPUs on ISIM or px_MessageAccountIdentity. UE shall use px_MessageAccountIdentity when that is configured to the phone as Public service identity of the message account.		
tag		not present		
Contact				RFC 3261 [15]
addr-spec	A1	SIP URI with IP address or FQDN and protected server port of UE		
addr-spec	A2	SIP URI with IP address or FQDN and unprotected server port of UE		
Expires				RFC 3261 [15]
delta-seconds		must be present but value not checked		
Security-Verify	A1			RFC 3329 [21]
sec-mechanism		same value as SecurityServer header sent by SS		
Require	A1			RFC 3261 [15] RFC 3329 [21]
option-tag		*sec-agree*		
Proxy-Require	A1			RFC 3261 [15] RFC 3329 [21]
option-tag		*sec-agree*		
CSeq				RFC 3261 [15]
value		must be present, value not checked		
method		*SUBSCRIBE*		
Call-ID				RFC 3261 [15]
callid		value not checked, but stored for later reference		
Session-ID	A3			draft-kaplan-dispatch-session-id [115]
sess-id		value not checked, but stored for later reference		

Header/param	Cond	Value/remark	Rel	Reference
Max-Forwards				RFC 3261 [15]
value		non-zero value		
P-Access-Network-Info	A1	(header optional when A2)		RFC 3455 [18]
access-net-spec		access network technology and, if applicable, the cell ID		
Accept				RFC 3261 [15] RFC 3842 [88]
media-range		*application/simple-message-summary*		
Event				RFC 3265 [34] RFC 3842 [88]
event-type		*message-summary*		
Content-Length				RFC 3261 [15]
value		length of request body, if such is present		

Condition	Explanation
A1	IMS security (A.6a/2)
A2	GIBA (A.6a/1)
A3	UE supports Session-ID(A.12/30 TS 34.229-2 [5])

NOTE 1: All choices for applicable conditions are described for each header.

A.6.2 NOTIFY for message-summary event package

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*NOTIFY*		
Request-URI		UE"s contact address in SIP URI form, as provided in the Contact header within the SUBSCRIBE creating the dialog		
SIP-Version		*SIP/2.0*		
Via		order of the parameters in this header must be like in this table		RFC 3261 [15]
via-parm1:				
Sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by	A1	IP address and protected server port of SS		
sent-by	A2	IP address and unprotected server port of SS (optional)		
via-branch		value starting with "*z9hG4bK"*		
via-parm2:				
sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by		px_scscf		
via-branch		value starting with "*z9hG4bK"*		
via-parm3:				
sent-protocol		*SIP/2.0/UDP* when using UDP or *SIP/2.0/TCP* when using TCP		
sent-by		px_MessageServerDomainName		
via-branch		value starting with "*z9hG4bK"*		
From				RFC 3261 [15]
addr-spec		any IMPU within the set of IMPUs on ISIM or px_MessageAccountIdentity. SS shall use px_MessageAccountIdentity when that is configured to the phone as Public service identity of the message account.		
tag		tag value corresponding to the SIP URI in the From header		
To				RFC 3261 [15]
addr-spec		any IMPU within the set of IMPUs on ISIM		
tag		tag value corresponding to the SIP URI in the To header		
Call-ID				RFC 3261 [15]
callid		same as value received in SUBSCRIBE message		
Session-ID				draft-kaplan-dispatch-session-id [115]
sess-id		same value as received in SUBSCRIBE message, if Session-ID header field exists in SUBSCRIBE message, otherwise, not present		
CSeq	A1,A2			RFC 3261 [15]
value		value of CSeq sent by the SS within its previous request in the same dialog but increased by one		
method		*NOTIFY*		
Contact				RFC 3261 [15]
addr-spec		px_MessageServerContactUri		
Content-Type				RFC 3261 [15] RFC 4575 [86]
media-type		*application/simple-message-summary*		
Event	A1,A2			RFC 3265[34] RFC 3842 [88]
event-type		*message-summary*		
Max-Forwards				RFC 3261 [15]
value		*69*		
Subscription-State				RFC 3265[34]
substate-value		*active*		

Header/param	Cond	Value/remark	Rel	Reference
expires		*7200*		
Content-Length value **Message-body**		 length of message-body *Messages-Waiting: no* *Message-Account:* **any IMPU within the set of IMPUs on ISIM** or **px_MessageAccountIdentity** as in From header		RFC 3261 [15] RFC 3842 [88]

Condition	Explanation
A1	IMS security (A.6a/2)
A2	GIBA (A.6a/1)

NOTE 1: All choices for applicable conditions are described for each header.

A.7 Default messages for SMS

A.7.1 MESSAGE for MT SMS

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*MESSAGE*		RFC 3428 [92]
Request-URI		UE"s registered contact address in SIP URI form, as provided in the Contact header of the REGISTER message		
SIP-Version		*SIP/2.0*		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP*		
sent-by		px_pcscf: protected server port of SS		
via-branch		value starting with "*z9hG4bK"*		
From				RFC 3261 [15]
addr-spec		SIP URI of the IP-SM-GW		
tag		any value		
To				RFC 3261 [15]
addr-spec		default public user identity of the UE		
tag		not present		
Call-ID				RFC 3261 [15]
callid		a random text string generated by the SS		
Session-ID	A1			draft-kaplan-dispatch-session-id [115]
sess-id		text string generated by the SS, SHA-1 hashing the Call-ID header value		
CSeq				RFC 3261 [15]
value		any value		
method		*MESSAGE*		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
Accept-Contact				RFC 3841 [64]
ac-value		*+g.3gpp.smsip;require;explicit*		
Request-Disposition				RFC 3841 [64]
fork-directive		*no-fork*		
P-Asserted-Identity				RFC 3325 [89]
addr-spec		SIP URI of the SS representing IP-SM-GW (same as in the From header)		
P-Called-Party-ID				RFC 3455 [18]
called-pty-id-spec		same value as in the To header		
Content-Type				RFC 3261 [15]
media-type		*application/vnd.3gpp.sms*		
Content-Length				RFC 3261 [15]
value		length of message-body		
Message-body		RP-DATA message including a SMS-DELIVER TPDU equal to - TP-MTI="00"B - TP-MMS="1"B (No more messages are waiting for the MS in this SC) - TP-RP=any allowed value - TP-OA=any allowed value - TP-PID=any allowed value - TP-DCS=any allowed value - TP-SCTS=any allowed value - TP-UDL=set according to length of TP-UD field - TP-UD=a valid SMS generated by SS		TS 24.011 [92] TS 23.040 [93]

Condition	Explanation
A1	UE supports Session-ID(A.12/30 TS 34.229-2 [5])

A.7.2 MESSAGE for delivery report for MT SMS

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version		 *MESSAGE* same P-Asserted-Identity URI as received in A.7.1 *SIP/2.0*		RFC 3261 [15] RFC 3428 [92] 3GPP TS 24.341
Via sent-protocol sent-by via-branch		 *SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP) not checked value starting with "*z9hG4bK"*		RFC 3261 [15]
From addr-spec tag		 SIP URI of the UE any value		RFC 3261 [15]
To addr-spec tag		 same as P-Asserted-Identity URI received in A.7.1 not present		RFC 3261 [15] 3GPP TS 24.341
Call-ID callid		 any value (but different from the Call-ID values used in preceding requests of this test case)		RFC 3261 [15]
In-Reply-to callid		 The value of the Call-Id received in the original MT SMS	Rel-11	RFC 3261 [15]
Session-ID sess-id		 same value as received in MESSAGE request, if Session-ID header field exists in MESSAGE request, otherwise, not present		draft-kaplan-dispatch-session-id [115]
CSeq value method		 any value *MESSAGE*		RFC 3261 [15]
Max-Forwards value		 non-zero value		RFC 3261 [15]
Content-Type media-type		 *application/vnd.3gpp.sms*		RFC 3261 [15]
Content-Length value		 length of message-body		RFC 3261 [15]
Message-body		RP-ACK message		TS 24.011 [92]

A.7.3 MESSAGE for MO SMS

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*MESSAGE*		RFC 3428 [91]
Request-URI		Public Service Identity of the SM-SC (default value as defined in E.3.2.15)		
SIP-Version		*SIP/2.0*		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP)		
sent-by		IP address or FQDN and protected server port of the UE		
via-branch		value starting with "*z9hG4bK"*		
From				RFC 3261 [15]
addr-spec		SIP URI of the UE		
tag		any value		
To				RFC 3261 [15]
addr-spec		Public Service Identity of the SM-SC (default value as defined in E.3.2.15)		
tag		not present		
Call-ID				RFC 3261 [15]
callid		must be present, value not checked		
Session-ID	A1			draft-kaplan-dispatch-session-id [115]
sess-id		must be present, value not checked		
CSeq				RFC 3261 [15]
value		any value		
method		*MESSAGE*		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
P-Access-Network-Info	A2	NOTE: header optional when A3		RFC 3455 [18]
access-net-spec		access network technology and, if applicable, the cell ID		
Route				RFC 3261 [15]
route-param		<sip:px_pcscf: protected server port of SS ;lr>, <sip:px_scscf;lr>		
Content-Type				RFC 3261 [15]
media-type		*application/vnd.3gpp.sms*		
Content-Length				RFC 3261 [15]
Value		length of message-body		
Message-body		RP-DATA message with RP-User Data set to SMS-SUBMIT type equal to - TP-MTI=" 01"B (SMS-SUBMIT) - TP-RD=any allowed value - TP-VPF=any allowed value - TP-RP=any allowed value - TP-MR=any allowed value - TP-DA=any allowed value - TP-PID=any allowed value - TP-DCS=any allowed value - TP-VP=any allowed value if TP-VPF indicates TP-VP field present; TP-VP=not present otherwise - TP-UDL=set according to length of TP-UD field - TP-UD=must be present and non-empty		TS 24.011 [92] TS 23.040 [93]

Condition	Explanation
A1	UE supports Session-ID (A.12/30 TS 34.229-2 [5])
A2	IMS security (A.6a/2 3GPP TS 34.229-2 [5])
A3	GIBA (A.6a/1 3GPP TS 34.229-2 [5])

A.7.4 MESSAGE for submission report for MO SMS

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version		 *MESSAGE* UE's registered contact address in SIP URI form, as provided in the Contact header of the REGISTER message *SIP/2.0*		RFC 3261 [15] RFC 3428 [91]
Via sent-protocol sent-by via-branch		 *SIP/2.0/UDP* px_pcscf: protected server port of SS value starting with "*z9hG4bK"*		RFC 3261 [15]
From addr-spec Tag		 SIP URI of the IP-SM-GW any value		RFC 3261 [15]
To addr-spec tag		 default public user identity of the UE must not be present		RFC 3261 [15]
Call-ID Callid		 any value (but different from the Call-ID values used in preceding requests of this test case)		RFC 3261 [15]
Session-ID sess-id		 same value as received in MESSAGE request, if Session-ID header field exists in MESSAGE request, otherwise, not present		draft-kaplan-dispatch-session-id [115]
In-Reply-to callid		 The value of the Call-Id received in the original MO SMS		RFC 3261 [15]
Cseq value method		 any value *MESSAGE*		RFC 3261 [15]
Max-Forwards Value		 non-zero value		RFC 3261 [15]
Request-Disposition fork-directive		 *f*ork		RFC 3261 [15]
P-Called-Party-ID value		 same value as in the To header		RFC 3455 [18]
P-Asserted-Identity value		 Public Service Identity of the SM-SC (default value as defined in E.3.2.15)		RFC 3325 [13]
Content-Type media-type		 *application/vnd.3gpp.sms*		RFC 3261 [15]
Content-Length Value		 length of message-body		RFC 3261 [15]
Message-body		RP-ACK message with RP-User Data including SMS-SUBMIT-REPORT: - TP-MTI="01"B (SMS-SUBMIT-REPORT) - TP-PI="00000000"B - TP-SCTS=set by the SS (encoded as specified in TS 23.040 clause 9.2.3.11)		TS 24.011 [92] TS 23.040 [93]

A.7.5 MESSAGE for status report for MO SMS

Header/param	Cond	Value/remark	Rel	Reference
Request-Line Method Request-URI SIP-Version		 *MESSAGE* UE's registered contact address in SIP URI form, as provided in the Contact header of the REGISTER message *SIP/2.0*		RFC 3261 [15] RFC 3428 [91]
Via sent-protocol sent-by via-branch		 *SIP/2.0/UDP* px_pcscf: protected server port of SS value starting with "*z9hG4bK"*		RFC 3261 [15] 3GPP TS 31.121 [113] 3GPP TS
From addr-spec Tag		 SIP URI of the IP-SM-GW any value		RFC 3261 [15]
To addr-spec tag		 default public user identity of the UE must not be present		RFC 3261 [15]
Call-ID Callid		 any value (but different from the Call-ID values used in preceding requests of this test case)		RFC 3261 [15]
Session-ID sess-id		 same value as received in MESSAGE request, if Session-ID header field exists in MESSAGE request, otherwise, not present		draft-kaplan-dispatch-session-id [115]
P-Asserted-Identity addr-spec		 Public Service Identity of the SM-SC (default value as defined in E.3.2.15)		RFC 3325 [89]
Cseq Value method		 Cseq value used in A.7.4 incremented by one *MESSAGE*		RFC 3261 [15]
Max-Forwards Value		 non-zero value		RFC 3261 [15]
Request-Disposition fork-directive		 no-fork		RFC 3261 [15]
Accept-Contact ac-value		 +g.3gpp.smsip;require;explicit		RFC 3841 [64]
Content-Type media-type		 *application/vnd.3gpp.sms*		RFC 3261 [15]
Content-Length Value		 length of message-body		RFC 3261 [15]
Message-body		RP-DATA message with RP-User Data including SMS-STATUS-REPORT: - TP-MTI="10"B (SMS-STATUS-REPORT) - TP-MMS="0"B - TP-SRQ="0"B - TP-MR=same value as that set by the UE in the RP-DATA of the MO SMS - TP-RA=same value as the TP-DA set by the UE in the RP-DATA of the MO SMS - TP-SCTS=same value as that set by the SS in the RP-ACK acknowledging the MO SMS - TP-DT=set by the SS (encoded as specified in TS 23.040 clause 9.2.3.11) - TP-ST="0000000"B (Short message received by the SME)		TS 24.011 [92]

A.7.6 MESSAGE for delivery report for MO SMS

Header/param	Cond	Value/remark	Rel	Reference
Request-Line				RFC 3261 [15]
Method		*MESSAGE*		RFC 3428 [92]
Request-URI		same as P-Asserted-Identity URI received in A.7.5		3GPP TS 24.341
SIP-Version		*SIP/2.0*		
Via				RFC 3261 [15]
sent-protocol		*SIP/2.0/UDP* (when using UDP) or *SIP/2.0/TCP* (when using TCP)		
sent-by		not checked		
via-branch		value starting with "*z9hG4bK"*		
From				RFC 3261 [15]
addr-spec		SIP URI of the UE		
tag		any value		
To				RFC 3261 [15]
addr-spec		Same as P-Asserted-Identity URI received in A.7.5		3GPP TS 24.341
tag		not present		
Call-ID				RFC 3261 [15]
callid		any value (but different from the Call-ID values used in preceding requests of this test case)		
In-Reply-to			Rel-11	RFC 3261 [15]
callid		The value of the Call-Id received in the status report for which this is a delivery report		
Session-ID				draft-kaplan-dispatch-session-id [115]
sess-id		same value as received in MESSAGE request, if Session-ID header field exists in MESSAGE request, otherwise, not present		
CSeq				RFC 3261 [15]
value		any value		
method		*MESSAGE*		
Max-Forwards				RFC 3261 [15]
value		non-zero value		
Content-Type				RFC 3261 [15]
media-type		*application/vnd.3gpp.sms*		
Content-Length				RFC 3261 [15]
value		length of message-body		
Message-body		RP-ACK message		TS 24.011 [92]

A.7.7 RP-DATA message (UE to Network)

Information element	Value/Remark
RP-Message Type	"000"B
RP-Message Reference	Any valid value
RP-Originator Address	0 length address
RP-Destination Address	TS-Service Centre Address(default value as defined in E.3.2.14)
RP-User Data	Any valid value

Annex B (normative): Default DHCP messages

For all the message definitions below, the acceptable order and syntax of headers and fields within these headers must be according to IETF RFCs where those headers have been defined. Typically the order of headers is not significant, but there are well defined exceptions where the order is important.

For IPv6 DHCP messages refer to RFC 3315[23].

For IPv4 DHCP messages refer to RFC 2131[55].

The contents of the messages described in the present Annex is not complete - only the fields and headers required to be checked or generated by SS are listed here. The messages sent by the UE may contain additional parameters, fields and headers which are not checked and must thus be ignored by SS.

B.1 Default DHCP messages (IPv6)

B.1.1 DHCP INFORMATION-REQUEST

Options	Value/Remarks
msg-type	INFORMATION-REQUEST (11)
transaction-id	Check If Present Note the Value to be included in Reply Message
option-code	OPTION_CLIENTID (1)
- option-len	Length of the DUID of Client
- DUID	Set to DUID of Client

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

B.1.2 DHCP REPLY

Options	Value/Remarks
msg-type	REPLY (7)
transaction-id	Set the same value as received in the corresponding Uplink Information Request message
option-code	OPTION_CLIENTID (1)
- option-len	Length of the DUID of client
- DUID	Set to DUID of Client
option-code	OPTION_SERVERID 21)
- option-len	Length of the DUID of Server
- DUID	Set to DUID of Server

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

B.1.3 DHCP SOLICIT

Options	Value/Remarks
msg-type	SOLICIT (1)
transaction-id	Check If Present Note the Value to be included in Reply Message
option-code	OPTION_CLIENTID (1)
- option-len	Length of the DUID of Client
- DUID	Set to DUID of Client
option-code	OPTION_ORO (6)
- option-len	Check Specific message contents in test case
- requested-option-code	Check Specific message contents in test case

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

B.1.4 DHCP ADVERTISE

Options	Value/Remarks
msg-type	ADVERTISE (2)
transaction-id	Set the same value as received in the corresponding Uplink solicit message
option-code	OPTION_CLIENTID (1)
- option-len	Length of the DUID of client
- DUID	Set to DUID of Client
option-code	OPTION_SERVERID (21)
- option-len	Length of the DUID of Server
- DUID	Set to DUID of Server

*NOTE: Numerical value, "(n)", provided in brackets in Column Value/Remarks is the 'octal' value for this option.

B.2 Default DHCP messages (IPv4)

B.2.1 DHCP DISCOVER

Fields	Value/Remarks
op	1 (BOOTREQUEST)
htype	Check if valid value is included
hlen	Check if valid value is included
hops	0
xid	Check For Presence Note the Value to be included in Offer Message
secs	Any Value
flags	Check For Presence Note the Value to be included in Offer Message
ciaddr	0
yiaddr	0
siaddr	0
giaddr	0
chaddr	FFS
sname	Options if indicated in sname/file else not used
file	Options if indicated in sname/file else not used
options - code - len - Type	* 53 (DHCP Message Type) 1 1 (DHCP DISCOVER)

* NOTE: Additional options may be present

B.2.2 DHCP OFFER

Fields	Value/Remarks
op	2 (BOOTREPLY)
htype	Set to SS Hardware Type
hlen	Set to SS Hardware Address Len
hops	0
xid	Set to same value as received in corresponding DISCOVER message
secs	0
flags	Set to same value as received in corresponding DISCOVER message
ciaddr	0
yiaddr	IP address of Mobile
siaddr	Set to IP address of next Boot Strap server
giaddr	Set to same value as received in corresponding DISCOVER message
chaddr	Set to same value as received in corresponding DISCOVER message
sname	Set to Server Host name
file	Set to Client Boot File Name
options	*
- code - len - Type	53 (DHCP Message Type) 1 2 (DHCP OFFER)

* NOTE: Additional options included in response to options requested by UE and supported by SS

B.2.3 DHCP INFORM

Fields	Value/Remarks
op	1 (BOOTREQUEST)
htype	Check if valid value is included
hlen	Check if valid value is included
hops	0
xid	Check For Presence Note the Value to be included in Offer Message
secs	Any Value
flags	Check For Presence Note the Value to be included in Offer Message
ciaddr	Set to UE"s Network address
yiaddr	0
siaddr	0
giaddr	0
chaddr	FFS
sname	Options if indicated in sname/file else not used
file	Options if indicated in sname/file else not used
options	*
- code - len - Type	53 (DHCP Message Type) 1 8 (DHCP INFORM)

* NOTE: Additional options may be present

B.2.4 DHCP ACK

Fields	Value/Remarks
op	2 (BOOTREPLY)
htype	Set to SS Hardware Type
hlen	Set to SS Hardware Address Len
hops	0
xid	Set to same value as received in corresponding INFORM message
secs	0
flags	Set to same value as received in corresponding INFORM message
ciaddr	0
yiaddr	IP address of Mobile
siaddr	Set to IP address of next Boot Strap server
giaddr	Set to same value as received in corresponding INFORM message
chaddr	Set to same value as received in corresponding INFORM message
sname	Set to Server Host name
file	Set to Client Boot File Name
options - code - len - Type	* 53 (DHCP Message Type) 1 5 (DHCP ACK)

* NOTE: Additional options included in response to options requested by UE

Annex C (normative): Generic Test Procedure

This Annex contains information about generic test procedures.

Annex A requirements for default messages apply.

SDP structured text denoted as (name), means the "name" field must be present but any value is allowed.

C.1 Introduction

This annex specifies general procedures for PDP context activation, EPS bearer context activation, P-CSCF discovery and IMS registration.

The annex includes also application specific procedures, e.g. for a MTSI client.

C.2 Generic Registration Test Procedure – IMS support

The generic test procedure:

1. EPS bearer context activation according annex C.18 for UE with E-UTRA support (TS 34.229-2 A.18/1). PDP context activation according annex C.17 for UE with UTRA support (TS 34.229-2 A.18/2) only.

3. Optional P-CSCF address discovery using the DHCP procedure according to Annex C.3 for IPv6 or Annex C.4 for IPv4.

4. The UE initiates IMS registration. SS waits for the UE to send an initial REGISTER request.

5. The SS responds to the initial REGISTER request with a valid 401 Unauthorized response.

6. The SS waits for the UE to set up a temporary set of security associations and to send another REGISTER request, over those security associations.

7. The SS responds to the second REGISTER request with valid 200 OK response, sent over the same temporary set of security associations that the UE used for sending the REGISTER request.

8. The SS waits for the UE to send a SUBSCRIBE request over the newly established security associations.

9. The SS responds to the SUBSCRIBE request with a valid 200 OK response.

10. The SS sends a valid NOTIFY request for the subscribed registration event package.

11. The SS waits for the UE to respond to the NOTIFY with a 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1				Annex C.17 or C.18.
2				Void.
3				Optional P-CSCF address discovery using the DHCP procedure according to Annex C.3 for IPv6 or Annex C.4 for IPv4.
4	→		REGISTER	The UE sends initial registration for IMS services.
5	←		401 Unauthorized	The SS responds with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network.
6	→		REGISTER	The UE completes the security negotiation procedures, sets up a temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials.
7	←		200 OK	The SS responds with 200 OK.
8	→		SUBSCRIBE	The UE subscribes to its registration event package.
9	←		200 OK	The SS responds with 200 OK.
10	←		NOTIFY	The SS sends initial NOTIFY for registration event package, containing full registration state information for the registered public user identity in the XML body
11	→		200 OK	The UE responds with 200 OK.

NOTE: The default message contents in annex A are used.

C.2a Generic Registration Test Procedure – GIBA

The generic test procedure:

1 EPS bearer context activation according annex C.18 for UE with E-UTRA support (TS 34.229-2 A.18/1). PDP context activation according annex C.17 for UE with UTRA support (TS 34.229-2 A.18/2) only.

2 void

3 Optional P-CSCF address discovery using the DHCP procedure according to Annex C.3 for IPv6 or Annex C.4 for IPv4.

4 The UE initiates IMS registration indicating support ofGIBA. SS waits for the UE to send an initial REGISTER request.

5 The SS responds to the REGISTER request with valid 200 OK response,

6 The SS waits for the UE to send a SUBSCRIBE request.

7 The SS responds to the SUBSCRIBE request with a valid 200 OK response.

8 The SS sends a valid NOTIFY request for the subscribed registration event package.

9 The SS waits for the UE to respond to the NOTIFY with a 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1				Annex C.17 or C.18.
2				Void.
3				Optional P-CSCF address discovery using the DHCP procedure according to Annex C.3 for IPv6 or Annex C.4 for IPv4.
4	→		REGISTER	The UE sends initial registration for IMS services indicating support for GIBA procedure by not including an Authorization header field.
5	←		200 OK	The SS responds with 200 OK.
6	→		SUBSCRIBE	The UE subscribes to its registration event package.
7	←		200 OK	The SS responds with 200 OK.
8	←		NOTIFY	The SS sends initial NOTIFY for registration event package, containing full registration state information for the registered public user identity in the XML body
9	→		200 OK	The UE responds with 200 OK.

NOTE: The default message contents in annex A are used.

C.3 Generic DHCP test procedure for IPv6

The generic test procedure (according to RFC 3315[23]):

1 The UE may send a DHCP SOLICIT message requesting to resolve P-CSCF Domain Name(s).

2 The SS responds with a DHCPADVERTISE message containing the IP address of the SS as P-CSCF address, if the UE requested the SIP Servers option within the DHCPSOLICIT message.

3 The UE may send a DHCP INFORMATION-REQUEST message if it has sent a DHCP SOLICIT message before. The UE shall send a DHCP INFORMATION-REQUEST if it has not sent a DHCP SOLICIT message before.

4 The SS responds with a DHCPREPLY message containing the IP address of the SS as P-CSCF address.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		DHCP SOLICIT	Optionally requesting to locate a DHCP server.
2	←		DHCPADVERTISE	Sent if the UE requested the SIP Servers option within the DHCPSOLICIT message.
3	→		DHCPINFORMATION-REQUEST	Optional message if DHCP SOLICIT was sent before, otherwise mandatory..
4	←		DHCPREPLY	Sent if DHCPINFORMATION-REQUEST is received.

NOTE: The default message contents in annex B are used.

C.4 Generic DHCP test procedure for IPv4

The generic test procedure (according to RFC 2131[55]):

1 If the UE already knows a DHCP server address, it goes to step 3. Otherwise, the UE sends a DHCPDISCOVER message locating a server.

2 The SS responds with a DHCPOFFER message.

3 The UE sends a DHCPINFORM message requesting P-CSCF address(es) in the options field.

4 The SS responds with a DHCPACK message providing the IP address of the SS as P-CSCF address.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		DHCPDISCOVER	Optionally sent if UE does not have DHCP server address.
2	←		DHCPOFFER	Sent if DHCP Discover message is received.
3	→		DHCPINFORM	Requesting P-CSCF Address(es).
4	←		DHCPACK	Including P-CSCF IP Address.

NOTE: The default message contents in annex B are used.

C.5 Default handling of PUBLISH requests

This procedure may occur at any time after a successful IMS registration.

The generic test procedure:

1 SS receives from the UE a PUBLISH request.

2 The SS responds to the PUBLISH request with a valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		PUBLISH	The UE sends a PUBLISH request (A.4.3).
2	←		200 OK	The SS responds with 200 OK (A.4.4).

NOTE: The default message contents in annex A are used.

C.6 Generic Secondary PDP Context test procedure

The generic test procedure may occur during establishment of a session. Applicable for a UE with UTRA support (TS 34.229-2 A.18/2) only.

1 The UE sends an Activate Secondary PDP Context Request message.

2 The SS responds with an Activate Secondary PDP Context Accept message.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		Activate Secondary PDP Context Request	The UE sends a request for an additional PDP context.
2	←		Activate Secondary PDP Context Accept	The SS responds with TI flag set to "1" and the TI value set to same as in step 1 in the linked TI information element.

C.7 Generic test procedure for setting up MTSI MO speech call

Editor"s note: The applicability of this annex is FFS.

The generic test procedure for setting up MTSI MO speech call may be performed after successful IMS or GIBA registration

1) MO call is initiated on the UE. The call is initiated towards the URI configured to SS as px_CalleeUri Depending on the UE support this URI may be either SIP or Tel URI, possibly containing a dialstring indicating a global, home local or geo-local telephone number. SS waits the UE to send an INVITE request with first SDP offer

2) SS responds to the INVITE request with a 100 Trying response.

3) SS responds to the INVITE request with a 183 Session in Progress response

4) SS waits for the UE to send a PRACK request possibly containing the second SDP offer.

5) SS responds to the PRACK request with valid 200 OK response.

6) SS waits for the UE to optionally send a UPDATE request containing the final SDP offer. UE will not send the UPDATE request if the PRACK in step 4 already contained the final offer with preconditions met.

7) SS responds to the UPDATE request (if UE sent one) with valid 200 OK response.

8) SS responds to the INVITE request with 180 Ringing response.

9) SS waits for the UE to send a PRACK request.

10) SS responds to the PRACK request with valid 200 OK response.

11. SS responds to the INVITE request with valid 200 OK response.

12) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		INVITE	UE sends INVITE with the first SDP offer indicating all desired medias and codecs the UE supports
2	←		100 Trying	The SS responds with a 100 Trying provisional response
3	←		183 Session in Progress	SS responds with an SDP answer only supporting AMR audio codec and indicating that SS has not yet reserved its resources.
4	→		PRACK	UE acknowledges the receipt of 183 response with PRACK and optionally offers second SDP that indicates preconditions as met
5	←		200 OK	The SS responds PRACK with 200 OK and answers the second SDP with mirroring its contents and indicates having reserved the resources if UE has also done so.
6	→		UPDATE	Optional step: UE sends an UPDATE after having reserved the resources with GPRS procedures for PDP context used for the media
7	←		200 OK	Optional step : The SS responds UPDATE with 200 OK and indicates having reserved the resources
8	←		180 Ringing	SS responds with 180 Ringing.
9	→		PRACK	UE acknowledges the receipt of 180 response by sending PRACK
10	←		200 OK	The SS responds PRACK with 200 OK
11	←		200 OK	The SS responds INVITE with 200 OK to indicate that the virtual remote UE had answered the call
12	→		ACK	The UE acknowledges the receipt of 200 OK for INVITE

Specific Message Contents

INVITE (Step 1)

Use the default message 'INVITE for MO call setup' in annex A.2.1 with the exception that Supported header shall contain the "precondition" tag. For the case of an emergency call either the condition A6 'INVITE for creating an emergency session in case of no registration' or A7 'INVITE for creating an emergency session within an emergency registration' shall apply, depending on whether the UE is equipped with UICC and has consequently performed an IMS registration. The UE shall include an SDP body with the following lines:

- All mandatory SDP lines, as specified in SDP grammar in RFC 4566 [27] appendix A, including:
  - "o=" line indicating e.g. the session identifier and the IP address of the UE;
  - "c=" line indicating the IP address of the UE for receiving the media flow for the session and/or media;
  - "b=" line proposing the application specific maximum bandwidth ("AS" modifier) for the session;
- Media description lines for the speech media proposed by UE for the MO call. For the offered speech media at least the following lines must exist within the SDP:
  - "m=" line describing the media type as audio, transport port and protocol used for media and media format as RTP/AVP;
  - "b=" line proposing the application specific maximum bandwidth ("AS" modifier) for the media;
  - "b=" line proposing the RTCP "RS" bandwidth modifier for the media. If the UE supports suppressing RTCP during the active two-way voice sessions, the UE shall offer the value as zero;
  - "b=" line proposing the RTCP "RR" bandwidth modifier for the media. If the UE supports suppressing RTCP during the active two-way voice sessions, the UE shall offer the value as zero;

- extra "a=" line for rtpmap attribute per each dynamic payload type given in the "m=" line. The UE shall offer at least the mandatory AMR codec; Additionally the UE shall offer telephone-events with event codes 0-15 if the UE supports sending DTMF events over RTP as specified in Annex G of TS 26.114 [66]..

- "a=" line for fmtp attribute per each rtpmap attribute. The fmtp attribute must cover at least the following parameters defined in RFC 4867 [67] for the AMR codec:
  mode-change-capability with value 2

- an "a=inactive" line

- four "a=" lines describing the current and desired state of the preconditions, as described in RFC 3312 [31]. At this stage of the call setup the lines shall be as follows:
  a=curr:qos local [none or sendrecv]
  a=curr:qos remote none
  a=des:qos mandatory local sendrecv
  a=des:qos optional remote sendrecv
  These four "a=" lines may appear in any order.

100 Trying for INVITE (Step 2)

Use the default message '100 Trying for INVITE' in annex A.2.2.

183 Session in Progress for INVITE (Step 3)

Use the default message '183 Session in Progress for INVITE' in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Require option-tag	*precondition*
Message-body	SDP body of the 183 response copied from the received INVITE but modified as follows: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; and - For speech media, the SS shall indicate only ARM codec and RTP/AVP to be supported. For all other media lines SS shall set the port number as zero in order to reject non-speech streams. - the "a=" lines describing the current and desired state of the preconditions, updated as follows: a=curr:qos local [none or sendrecv] (* a=curr:qos remote [none or sendrecv] (* a=des:qos mandatory local sendrecv a=des:qos mandatory remote sendrecv a=conf:qos remote sendrecv *) The value of these direction-tags in 183 must be none if the UE has not yet reserved its resources, but otherwise sendrecv

For the case of an emergency call the condition A5 '183 sent by the SS for INVITE for creating an emergency session' shall apply

PRACK (Step 4)

Use the default message 'PRACK' in annex A.2.4 with the exception that either Supported or Require header shall contain the "precondition" tag. The UE may include a SDP body in the PRACK request to indicate it has met the preconditions. In that case the following lines shall be included in the SDP body of PRACK:

- All mandatory SDP lines are present, as specified in SDP grammar in RFC 4566 [27] appendix A; and

- "o" line shall be the same like in INVITE request, except that the version number shall be increased; and
- "b=" line proposing the application specific maximum bandwidth ("AS" modifier) for the session; and
- "b=" line proposing the application specific maximum bandwidth ("AS" modifier) for the media; and
- "b=" line proposing the RTCP "RS" bandwidth modifier for the media. If the UE supports suppressing RTCP during the active two-way voice sessions,, the UE shall offer the value as zero; and
- "b=" line proposing the RTCP "RR" bandwidth modifier for the media. If the UE supports suppressing RTCP during the active two-way voice sessions,, the UE shall offer the value as zero; and
- SDP must contain at least as many media description lines as the SDP in the INVITE contained. One of them must be for speech media with AMR codec supported by the SS and the other for telephone-events if included to the original offer in step 1; and
- four "a=" lines describing the current and desired state of the preconditions, as described in RFC 3312 [31]. At this stage of the call setup the lines shall be as follows:
  a=curr:qos local sendrecv
  a=curr:qos remote none
  a=des:qos mandatory local sendrecv
  a=des:qos optional remote sendrecv
  These four "a=" lines may appear in any order.
- as the UE has met its local preconditions the a=inactive line must be replaced with a=sendrecv line.

200 OK for PRACK (Step 5)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	header shall be present only if there is SDP in message-body *application/sdp*
Content-Length value	 length of message-body
Message-body	SDP body of the 200 response copied from the received PRACK, if it contained one but otherwise omitted. The copied SDP body must be modified as follows for the 200 OK response: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; and - For speech media, the SS shall indicate only ARM codec and RTP/AVP to be supported. For all other media lines SS shall set the port number as zero in order to reject non-speech streams. - the "a=" lines describing the current and desired state of the preconditions, as described in RFC 3312 [31], updated as follows: a=curr:qos local sendrecv a=curr:qos remote sendrecv a=des:qos mandatory local sendrecv a=des:qos mandatory remote sendrecv

UPDATE (Step 6) optional step used when PRACK contained a=curr:qos local none

Use the default message 'UPDATE' in annex A.2.5 with the exception that either Supported or Require header shall contain the "precondition" tag. The UE must include a SDP body in the UPDATE request to indicate it has met the preconditions. The following lines shall be included in the SDP body:

- All mandatory SDP lines are present, as specified in SDP grammar in RFC 4566 [27] appendix A; and

- "o" line shall be the same like in INVITE request, except that the version number shall be increased; and
- "b=" line proposing the application specific maximum bandwidth ("AS" modifier) for the session; and
- "b=" line proposing the application specific maximum bandwidth ("AS" modifier) for the media; and
- "b=" line proposing the RTCP "RS" bandwidth modifier for the media. If the UE supports suppressing RTCP during the active two-way voice sessions, the UE shall offer the value as zero; and
- "b=" line proposing the RTCP "RR" bandwidth modifier for the media. If the UE supports suppressing RTCP during the active two-way voice sessions, the UE shall offer the value as zero; and
- SDP must contain at least as many media description lines as the SDP in the INVITE contained. One of them must be for speech media with AMR codec supported by the SS and the other for telephone-events if included to the original offer in step 1; and
- four "a=" lines describing the current and desired state of the preconditions, as described in RFC 3312 [31]. At this stage of the call setup the lines shall be as follows:
  a=curr:qos local sendrecv
  a=curr:qos remote none
  a=des:qos mandatory local sendrecv
  a=des:qos optional remote sendrecv
  These four "a=" lines may appear in any order.
- as the UE has met its local preconditions the a=inactive line must be replaced with a=sendrecv line.

200 OK for UPDATE (Step 7) - optional step used when UE sent UPDATE

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	**Value/remark**
Content-Type media-type	 *application/sdp*
Content-Length value	 length of message-body
Message-body	SDP body of the 200 response copied from the received UPDATE but modified as follows: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; and - For speech media, the SS shall indicate only ARM codec and RTP/AVP to be supported. For all other media lines SS shall set the port number as zero in order to reject non-speech streams. - the "a=" lines describing the current and desired state of the preconditions, as described in RFC 3312 [31], updated as follows: a=curr:qos local sendrecv a=curr:qos remote sendrecv a=des:qos mandatory local sendrecv a=des:qos mandatory remote sendrecv

180 Ringing for INVITE (Step 8)

Use the default message '180 Ringing for INVITE' in annex A.2.6. For the case of an emergency call the condition A4 '180 sent by the SS when setting up an emergency call' shall apply.

PRACK (Step 9)

Use the default message 'PRACK' in annex A.2.4.

200 OK for PRACK (Step 10)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

200 OK for INVITE (Step 11)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1. For the case of an emergency call the condition A6 'Response sent by SS for INVITE for emergency call' shall apply

ACK (Step 12)

Use the default message 'ACK' in annex A.2.7.

C.8 Generic test procedure for putting a MTSI speech call to hold or to resume the call from the UE

The generic test procedure for putting a MTSI speech call to hold may be performed while MTSI speech call is going on

Test procedure

1) SS waits the UE to send an INVITE or UPDATE request with a SDP offer
2) If UE sent an INVITE request in step 1, SS responds to the it with a 100 Trying response. No such response is sent for UPDATE.
3) SS responds to the INVITE or UPDATE request with valid 200 OK response.
4) If UE sent an INVITE in step 1 SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		INVITE or UPDATE	UE sends INVITE or UPDATE with a SDP offer to hold or resume the call
2	←		100 Trying	Optional: The SS responds to the INVITE with a 100 Trying provisional response
3	←		200 OK	The SS responds INVITE or UPDATE with 200 OK to indicate that the remote UE is no more sending any media (call hold) or resumes sending media (call resume)
4	→		ACK	Optional: If the UE sent INVITE in step 1 then UE acknowledges the receipt of 200 OK for INVITE

Specific Message Contents

INVITE or UPDATE (Step 1)

Use the default message 'INVITE for MO call setup' in annex A.2.1 or 'UPDATE' in annex A.2.5. In case of an INVITE the UE shall use also the same URI in the request line as the SS has sent in the Contact header of an earlier message within the same dialog (in case of an UPDATE ref. to A.2.5).

The UE shall include the same lines in the SDP body as in its previous offer but with the following exceptions:

- Version number of the SDP shall be increased; and

  - - in case of Call Hold

  - If the UE supports sending RTCP while the call is being hold, it shall add a "b=" line for the RTCP "RS" bandwidth modifier, proposing a value greater than zero; and

  - If the UE supports sending RTCP while the call is being hold, it shall add a "b=" line for the RTCP "RR" bandwidth modifier, proposing a value greater than zero; and

  - - in case of Call Resume

  - if the UE suppresses RTCP during the active two-way voice sessions, the values of RTCP "RR" and 'RS' bandwidth modifiers shall be returned back to zero.

- the UE shall either add a session level direction attribute (and remove the direction attributes of all the media lines) or modify the direction attributes of all the media lines as follows:

  - - in case of Call Hold

  - If the directionality of the media lines were originally as "recvonly" then the directionality attributes within the INVITE in step 1 shall be "inactive"

  - If the directionality of the media lines were originally as "sendrecv" then the directionality attributes within the INVITE in step 1 shall be "sendonly"

  - - in case of Call Resume

  - the UE shall restore the value of the directionality attributes within the SDP body their original values (the UE may use either a single session level attribute or separate attributes for each media line).

100 Trying for INVITE (Step 2) optional step used when UE sent INVITE in step 1

Use the default message '100 Trying for INVITE' in annex A.2.2.

200 OK for INVITE or UPDATE (Step 3)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Message-body	SDP body of the 200 OK response copied from the received INVITE or UPDATE but modified as follows: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should send the media; and In case of Call Hold: - every "sendonly" directionality attribute inverted to "recvonly"

ACK (Step 4) optional step used when UE sent INVITE in step 1

Use the default message 'ACK' in annex A.2.7.

C.9 Generic test procedure for putting a MTSI speech call to hold from the SS

The generic test procedure for putting a MTSI speech call to hold may be performed while MTSI speech call is going on

1) SS initiates the call hold by sending a re-INVITE to set the media streams into sendonly state.
2) Optional: SS waits for the UE to respond to the INVITE request with a 100 Trying response.
3) SS waits for the UE to respond to the INVITE request with valid 200 OK response.
4) SS sends an ACK to acknowledge receipt of the 200 OK for INVITE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with a SDP offer indicating all medias as sendonly
2	→		100 Trying	Optional: The UE responds with a 100 Trying provisional response
3	→		200 OK	The UE responds INVITE with 200 OK to indicate that the UE is no more expecting to receive any media
4	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE

Specific Message Contents

INVITE (Step 1)

Use the default message 'INVITE for MT call setup' in annex A.2.9 with the following exceptions:

The SS shall include the same lines in the SDP body as finally accepted for the MTSI call but change the directionality of all media lines as "sendonly". The values of 'RS' and 'RR' bandwidth modifiers shall be greater than zero. Version number of the SDP must be incremented by one compared to the previous SDP sent by the SS.

100 Trying for INVITE (Step 2)

Use the default message '100 Trying for INVITE' in annex A.2.2.

200 OK for INVITE (Step 3)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Message-body	Properly generated SDP answer to the SDP offer contained in the INVITE including: - All mandatory SDP lines as specified in RFC 4566[27]. - The same number of media lines ('m=') as in the INVITE. - All the media lines having directionality as "recvonly" - The values of 'RS' and 'RR' bandwidth modifiers shall be greater than zero if the UE supports sending RTCP while the call is being hold.

ACK (Step 4)

Use the default message 'ACK' in annex A.2.7.

C.10 Generic test procedure for MTSI conference creation

The generic test procedure for creating MTSI conference may be performed after successful IMS or early IMS registration

Test procedure

1-7) UE creates the voice conference. The same message sequence as in steps 1 - 7 of Annex C.7 are used to create the conference into the conference focus and negotiate the media.

8) SS responds to the INVITE request with valid 200 OK response.

9) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

10) SS waits the UE to optionally subscribe to the conference event package with a SUBSCRIBE message

11) If UE sent SUBSCRIBE, SS responds to it with 200 OK response.

12) If UE sent SUBSCRIBE, SS sends a NOTIFY for the conference event package to the UE.

13) If SS sent a NOTIFY, SS waits the UE to respond the NOTIFY with 200 OK.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-7			Steps 1-7 of Annex C.7	The same messages as in steps 1 - 7 of Annex C.7
8	←		200 OK	The SS responds INVITE with 200 OK and gives the final conference URI within the response
9	→		ACK	The UE acknowledges the receipt of 200 OK for INVITE
10	→		SUBSCRIBE	Optional: UE subscribes the conference event
11	←		200 OK	Optional: SS responds to the subscription
12	←		NOTIFY	Optional: SS sends the initial state of the conference event to the UE
13	→		200 OK	Optional: UE responds to the NOTIFY

NOTE: The default messages contents in annex A are used with condition 'IMS security' or 'early IMS security' when applicable

Specific Message Contents

The specific message contents for steps 1 - 7 is otherwise identical to what has been specified in Annex C.7, but with the additional exceptions to steps 1 and 3 as below:

INVITE (Step 1)

Header/param	Value/remark
Request-Line	
Request-URI	px_ConferenceFactoryUri
To	
addr-spec	px_ConferenceFactoryUri

183 Session in Progress for INVITE (Step 3)

Header/param	Value/remark
Contact	
addr-spec	px_TemporaryConferenceUri
feature-param	*isfocus*

200 OK for INVITE (Step 8)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1

ACK (Step 9)

Use the default message 'ACK' in annex A.2.7.

SUBSCRIBE (Step 10)

Use the default message 'SUBSCRIBE for conference event package' in annex A.5.1.

200 OK for SUBSCRIBE (Step 11)

Use the default message '200 OK for SUBSCRIBE' in annex A.5.2.

NOTIFY (Step 12)

Use the default message 'NOTIFY for conference event package' in annex A.5.3.

200 OK for NOTIFY (Step 13)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

C.11 Generic test procedure for setting up MTSI MT speech call

The generic test procedure for setting up MTSI MT speech call may be performed after successful IMS or early IMS registration.

Test procedure

1) SS sends an INVITE request to the UE.
2) Void.
3) SS may receive 100 Trying from the UE.
4) SS expects and receives 183 Session Progress from the UE.
5) SS sends PRACK to the UE to acknowledge the 183 Session Progress.
6) SS expects and receives 200 OK for PRACK from the UE.
7) SS sends UPDATE to the UE, with SDP indicating that precondition is met on the server side.
8) SS expects and receives 200 OK for UPDATE from the UE, with proper SDP as answer.
9) SS may receive 180 Ringing from the UE.
10) SS may send PRACK to the UE to acknowledge the 180 Ringing.
11) SS may receive 200 OK for PRACK from the UE.

11A) The UE accepts the session invite.

12) SS expects and receives 200 OK for INVITE from the UE.
13) SS sends ACK to the UE.
14) SS sends BYE to the UE.
15) SS expects and receives 200 OK for BYE from the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with the first SDP offer.
2				Void
3	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response
4	→		183 Session Progress	The UE sends 183 response reliably with the SDP answer to the offer in INVITE
5	←		PRACK	SS acknowledges the receipt of 183 response from the UE.
6	→		200 OK	The UE responds to PRACK with 200 OK.
7	←		UPDATE	SS sends an UPDATE with SDP offer indicating SS reserved resources.
8	→		200 OK	The UE acknowledges the UPDATE with 200 OK and includes SDP answer to acknowledge its current precondition status.
9	→		180 Ringing	(Optional) The UE responds to INVITE with 180 Ringing.
10	←		PRACK	(Optional) SS shall send PRACK only if the 180 response contains 100rel option tag within the Require header.
11	→		200 OK	(Optional) The UE acknowledges the PRACK with 200 OK.
11A				Make UE accept the speech AMR offer.
12	→		200 OK	The UE responds to INVITE with a 200 OK final response after the user answers the call.
13	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.
14	←		BYE	The SS sends BYE to release the call.
15	→		200 OK	The UE sends 200 OK for the BYE request and ends the call.

NOTE: The default messages contents in annex A are used with condition 'IMS security' or 'early IMS security' when applicable

Specific Message Content

INVITE (Step 1)

Use the default message 'INVITE for MT Call' in annex A.2.9 with the following exceptions:

Header/param	Value/remark
Supported option-tag	 *precondition* [Note 1]
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97* - *b=AS:30* - *b=RS:0* - *b=RR:2500* Attributes for media: - *a=rtpmap:97 AMR/8000/1* - *a=fmtp:97 mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Note 1: and additionally the option-tag carried over from A2.9

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/remark
Status-Line	
Reason-Phrase	Not checked
Require	
option-tag	*precondition* [Note 2]
Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o*=(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 3] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 3] - *a=fmtp:*(format) [Note 3, 4] Attributes for preconditions: - *a=curr:qos local none* or *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: and additionally the option-tag carried over from A2.9 Note 3: The value for fmt, payload type and format is not checked Note 4: Parameters for the AMR codec are not checked

UPDATE (step 7)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111112 IN* (addrtype) (unicast-address for SS) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97* - *b=AS:30* - *b=RS:0* - *b=RR:2500* Attributes for media: - *a=rtpmap:97 AMR/8000* [Note 2] - *a=fmtp:97 mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* - *a=sendrecv* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* or *curr:qos remote sendrecv* [Note 1] - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: Use the value (none/sendrecv) received from 183 Session Progress and attribute a=curr:qos local. Note 2: The AMR channel number shall be '/1' or omitted.

200 OK (step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type	
media-type	*application/sdp*
Content-Length	
value	length of message-body

Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o=*(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=*(session *name)* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 2] - *a=fmtp:*(format) [Note 2, 3] - *a=sendrecv* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The value for fmt, payload type and format is not checked Note 3: Parameters for the AMR codec are not checked

C.12 Void

C.13 Generic test procedure for setting up MTSI MT text call

The generic test procedure for setting up MTSI MT text call may be performed after successful IMS or early IMS registration.

Test procedure

1) SS sends an INVITE request to the UE.

2) Void

3) SS may receive 100 Trying from the UE.

4) SS may receive 180 Ringing from the UE.

5) SS may send PRACK to the UE to acknowledge the 180 Ringing.

6) SS may receive 200 OK for PRACK from the UE.

6A) The UE accepts the session invite.
If 180 Ringing is not received from the UE after 5s from step 1, the MMI command shall be started to trigger the UE to accept the call.

7) SS receives 200 OK for INVITE from the UE.

8) SS send an ACK to acknowledge receipt of the 200 OK for INVITE

9) SS sends BYE to the UE.

10) SS expects and receives 200 Ok for BYE from the UE

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with the first SDP offer.
2				Void
3	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response.
4	→		180 Ringing	(Optional) The UE responds to INVITE with 180 Ringing.
5	←		PRACK	(Optional) SS shall send PRACK if the 180 response contains 100rel option-tag in the Require header.
6	→		200 OK	(Optional) The UE acknowledges the PRACK with 200 OK.
6A				Make UE accept the speech AMR offer.
7	→		200 OK	The UE responds INVITE with 200 OK.
8	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.
9	←		BYE	The SS releases the call with BYE.
10	→		200 OK	The UE sends 200 OK for BYE.

NOTE: The default messages contents in annex A are used with condition 'IMS security ' or 'early IMS security' when applicable

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9, with the following exceptions:

Header/param	Value/Remark
Supported option-tag	*precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o= - 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:3* Time description: - *t=0 0* Media description: - *m=text* (transport port) *RTP/AVP 99 101* - *b=AS:3* - *b=RS:0* - *b=RR:500* Attributes for media: - *a=rtpmap:99 t140/1000* - *a=rtpmap:101 red/1000* - *a=fmtp:101 99/99/99* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

100 Trying for INVITE (Step 3)

Use the default message '100 Trying for INVITE' in annex A.2.2

180 Ringing (Step 4)

Use the default message '180 Ringing for INVITE' in annex A.2.6 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	Header optional Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o=*(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=(session name)* - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=text* (transport port) *RTP/AVP* (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap*:(payload type) *t140/1000* [NOTE 2] - *a=rtpmap*:(payload type) *red/1000* [NOTE 2] - *a=fmtp:*(format) [NOTE 2] Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: values in fmt and values for payload type and format are not checked

PRACK (step 5)

Use the default message "PRACK" in annex A.2.4. No content body is included in this PRACK message

200 OK (Step 6)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

200 OK for INVITE (Step 7)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	Contents if header Content-Type is present: length of message-body
Message-body	Header not present if 180 Ringing (step 4) contained SDP. Header present if 180 Ringing (step 4) did not contain SDP. Contents if present: The same requirements for SDP types and values as specified in step 4.

ACK (Step 8)

Use the default message 'ACK' in annex A.2.7.

BYE (step 9)

Use the default message "BYE" in annex A.2.8.

200 OK (step 10)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

C.14 Default handling of SUBSCRIBE requests for MWI

This procedure may occur at any time after a successful IMS registration.

The generic test procedure:

1 SS receives from the UE a SUBSCRIBE request for Message Waiting Indication package.

2 The SS responds to the SUBSCRIBE request with a valid 200 OK response.

3. SS sends UE a NOTIFY request for the subscribed Message Waiting Indication event package referring to no messages waiting.

4. SS waits for the UE to respond the NOTIFY with 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		SUBSCRIBE	UE subscribes to the Message Waiting Indication event package (A.6.1).
2	←		200 OK	The SS responds SUBSCRIBE with 200 OK (A.1.5)
3	←		NOTIFY	The SS sends initial NOTIFY for Message Waiting Indication event package (A.6.2).
4	→		200 OK	The UE responds the NOTIFY with 200 OK (A.3.1)

NOTE: The default message contents in annex A are used.

C.15 Generic test procedure for setting up MTSI MO text call

The generic test procedure for setting up MTSI MT text call may be performed after successful IMS or early IMS registration.

Test procedure

1) Make UE initiate text.

2) UE sends an INVITE request.

3) SS responds to the INVITE request with a 100 Trying response.

4) SS responds to the INVITE request with 180 Ringing response.

5) SS responds to the INVITE request with valid 200 OK response.

6) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

7) Call is released on the UE. SS waits the UE to send a BYE request.

8) SS responds to the BYE request with valid 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1				Make UE initiate the text offer.
2	→		INVITE	UE sends INVITE with a SDP offer
3	←		100 Trying	The SS responds with a 100 Trying provisional response
4	←		180 Ringing	The SS responds INVITE with 180 Ringing to indicate that the remote UE has started ringing.
5	←		200 OK	The SS responds INVITE with 200 OK
6	→		ACK	The UE acknowledges the receipt of 200 OK for INVITE
7	→		BYE	The UE releases the call with BYE
8	←		200 OK	The SS sends 200 OK for BYE

NOTE: The default messages contents in annex A are used with condition 'IMS security ' or 'early IMS security' when applicable

Specific Message Contents

INVITE (Step 2)

Use the default message "INVITE for MO Call" in annex A.2.1, with the following exceptions:

Header/param	Value/remark
Supported option-tag	 *precondition*
Message-body	The following SDP types and values shall be present. Session description: - *v=* (protocol version) - *o=*(username) (sess-id) (sess-version) *IN IP4* or *IP6* (unicast-address for UE) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *s=* (session name) - *b=AS:* (bandwidth-value) Time description: - *t=* (time the session is active) Media description: - *m=text* (transport port) *RTP/AVP* (media format description) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap*:(payload type) *t140/1000* - *a=rtpmap*:(payload type) *red/1000* - *a=fmtp:*(format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Note 1: At least one "c=" field shall be present.

100 Trying for INVITE (Step 3)

Use the default message '100 Trying for INVITE' in annex A.2.2.

180 Ringing for INVITE (Step 4)

Use the default message '180 Ringing for INVITE' in annex A.2.6.

200 OK for INVITE (Step 5)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	**Value/remark**
Content-Type media-type	 *application/sdp*
Content-Length value	 length of message-body
Message-body	The following SDP types and values. The IP address on "o=" and "c=" lines and transport port on "m=" lines indicates to which IP address and port the UE should start sending the media. Use same values as received in step 2 for sess-id, sess-version, addrtype, session name, bandwidth-value (four places), media format description, payload type and format. Session description: - *v=0* - *o=-* (sess-id) (sess-version) *IN* (addrtype) (unicast-address for SS) - *c=IN* (addrtype) (connection-address for SS) - *s=*(session name) - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=text* (transport port) *RTP/AVP* (media format description) - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap*:(payload type) *t140/1000* - *a=rtpmap*:(payload type) *red/1000* - *a=fmtp:*(format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv*

ACK (Step 6)

Use the default message 'ACK' in annex A.2.7.

BYE (Step 7)

Use the default message 'BYE' in annex A.2.8.

200 OK for BYE (Step 8)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

C.16 Generic test procedure for setting up MTSI MT speech call, SS resources available

The generic test procedure for setting up MTSI MT speech call, SS resources available may be performed after successful IMS or early IMS registration.

Test procedure

1) SS sends an INVITE request to the UE.

2) The UE accepts the session invite.

3) SS may receive 100 Trying from the UE.

4) SS may receive 180 Ringing from the UE.

5) SS may send PRACK to the UE to acknowledge the 180 Ringing.

6) SS may receive 200 OK for PRACK from the UE.

7) SS expects and receives 200 OK for INVITE from the UE, with proper SDP as answer.

8) SS sends an ACK to acknowledge receipt of the 200 OK for INVITE

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with the first SDP offer.
2				Make UE accept the speech AMR offer.
3	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response.
4	→		180 Ringing	(Optional) The UE responds to INVITE with 180 Ringing.
5	←		PRACK	(Optional) SS shall send PRACK if the 180 response contains 100rel option-tag in the Require header.
6	→		200 OK	(Optional) The UE acknowledges the PRACK with 200 OK.
7	→		200 OK	The UE responds INVITE with 200 OK.
8	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.

NOTE: The default messages contents in annex A are used with condition 'IMS security ' or 'early IMS security' when applicable

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MT Call" in annex A.2.9, with the following exceptions:

Header/param	Value/Remark
Supported option-tag	*precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=IMS conformance test* - *c=IN (addrtype) (connection-address for SS)* - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97* - *b=AS:30* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=tcap:1 RTP/AVPF* - *a=pcfg:1 t=1* - *a=rtpmap:97 AMR/8000/1* - *a=fmtp:97 mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv*

100 Trying for INVITE (Step 3)

Use the default message '100 Trying for INVITE' in annex A.2.2

180 Ringing (Step 4)

Use the default message '180 Ringing for INVITE' in annex A.2.6 without the 'Record-Route' header and with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	Contents if header Content-Type is present: length of message-body
Message-body	Header optional Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o=*(user-name) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=*(session *name)* - *c=IN (addrtype) (connection-address for UE)* [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVPF* or *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=acfg:1 t=1* [Note 2] - *a=rtpmap:*(payload type) *AMR/8000* [Note 3] - *a=fmtp:*(format) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: Attribute acfg shall be present if *RTP/AVPF* is selected. Note 3: The AMR channel number shall be '/1' or omitted.

PRACK (step 5)

Use the default message "PRACK" in annex A.2.4. No content body is included in this PRACK message

200 OK (Step 6)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

200 OK for INVITE (Step 7)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length value	Contents if header Content-Type is present: length of message-body
Message-body	Header not present if 180 Ringing (step 4) contained SDP. Header present if 180 Ringing (step 4) did not contain SDP. Contents if present: The same requirements for SDP types and values as specified in step 4.

ACK (Step 8)

Use the default message 'ACK' in annex A.2.7.

C.17 PDP context activation

The procedure is applicable for a UE with UTRA support (TS 34.229-2 A.18/2) only.

The generic test procedure:

1 The UE sends an Activate PDP Context Request message. In the Protocol Configuration Options IE the IM CN Subsystem Signalling Flag may be set or not set, a request for P-CSCF Address or a request for DNS Server Address may be included or not.

2 The SS responds with an Activate PDP Context Accept message. In the Protocol Configuration Options IE the IM CN Subsystem Signalling Flag shall not be set, a list of P-CSCF addresses or DNS Server addresses shall only be included if a corresponding request was included in step 1.

NOTE: The required radio bearer(s) are established. For UMTS FDD they are established using RADIO BEARER SETUP (according to 3GPP TS 25.331 [58]).

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		Activate PDP Context Request	In the Protocol Configuration Options IE the IM CN Subsystem Signalling Flag may be set or not set, a request for P-CSCF Address or a request for DNS Server Address may be included or not.
2	←		Activate PDP Context Accept	In the Protocol Configuration Options IE the IM CN Subsystem Signalling Flag shall not be set, a list of P-CSCF IP addresses or DNS Server addresses shall only be included if a corresponding request was included in step 1.

NOTE: The default message contents in annex A are used with condition 'IMS AKA security ' or 'GIBA' when applicable.

C.18 EPS bearer context activation

The procedure is applicable for a UE with E-UTRA support (TS 34.229-2 A.18/1) only.

The generic test procedure:

1-17 Refer to TS 36.508 [94] subclause 4.5.2.3.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1-17				Registration procedure according TS 36.508 [94] subclause 4.5.2.3.

C.19 Generic test procedure for Inviting user to conference by sending a REFER request to the conference focus

The generic test procedure for Inviting user to conference by sending a REFER request to the conference focus may be performed after successful IMS or early IMS registration.

Test procedure

1) UE invites a user to the conference created. SS waits the UE to send to the conference focus a REFER request, which refers to the user to be invited to the conference.

2) SS responds to the REFER request with a valid 202 Accepted response.

3) SS sends an initial NOTIFY to tell that the invited user is trying to join the conference.

4) UE responds to the NOTIFY request with valid 200 OK response.

5) SS sends the final NOTIFY to tell that the invited user has successfully joined the conference.

6) UE responds to the NOTIFY request with a valid 200 OK response.

7) Optional: If UE subscribed the conference event package during the generic test procedure of Annex C.10, SS sends a NOTIFY for the conference event package to the UE to notify that the user joined the conference.

8) If SS sent a NOTIFY, SS waits the UE to respond the NOTIFY with 200 OK.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REFER	UE sends REFER to SS referring to the conference
2	←		202 Accepted	The SS responds with a 202 final response
3	←		NOTIFY	The SS sends initial NOTIFY for the implicit subscription created by the REFER request
4	→		200 OK	The UE responds the NOTIFY with 200 OK
5	←		NOTIFY	The SS sends a NOTIFY related to REFER request to confirm that the invited user was able to join the conference
6	→		200 OK	The UE responds the NOTIFY with 200 OK
7	←		NOTIFY	Optional: If the UE has subscribed the conference event package, the SS sends a NOTIFY for conference event package to inform that the invited user was able to join the conference
8	→		200 OK	Optional: The UE responds the NOTIFY with 200 OK

REFER (Step 1)

Use the default message 'MO REFER' in annex A.2.10 with the following exceptions:

Header/param	Value/remark
Request-URI	px_FinalConferenceUri
Refer-To	
addr-spec	SIP URI of the user invited to the conference
To	
addr-spec	px_FinalConferenceUri
tag	no tag given
Call-ID	
callid	value different to that received in INVITE message used to create the conference
CSeq	
value	must be present, value not checked

202 Accepted for REFER (Step 2)

Use the default message '202 Accepted' in annex A.3.3.

NOTIFY (Step 3)

Use the default message 'MT NOTIFY for refer package' in annex A.2.11 with the following exceptions:

Header/param	Value/remark
Message-body	*SIP/2.0 100 Trying*

200 OK for NOTIFY (Step 4)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

NOTIFY (Step 5)

Use the default message 'MT NOTIFY for refer package' in annex A.2.11 with the following exceptions:

Header/param	Value/remark
Subscription-State	
substate-value	*terminated*
expires	omitted from the request
reason	*noresource*
Message-body	*SIP/2.0 200 OK*

200 OK for NOTIFY (Step 6)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

NOTIFY (Step 7)

Use the default message 'NOTIFY for conference event package' in annex A.5.3 with the following exceptions:

Header/param	Value/remark
Message-body	*<?xml version="1.0" encoding="UTF-8"?>* *<conference-info xmlns="urn:ietf:params:xml:ns:conference-info">* *entity="***px_FinalConferenceUri***"* *state="partial"* *version="1"* *<users>* *<user entity="* **SIP URI of the invited user***">* *<endpoint entity="* **Contact URI of the invited user***">* *<status>connected</status>* *<joining-method>dialed-in</joining-method>* *<media id="1">* *<type>audio</type>* *<label>11223</label>* *<src-id>***random SSRC value***</src-id>* *<status>sendrecv</status>* *</media>* *</endpoint>* *</users>* *</conference-info>*

200 OK for NOTIFY (Step 8)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

C.20 Generic Test Procedure for IMS emergency registration

Test procedure:

1) SS waits for the UE to send an initial REGISTER request.
2) The SS responds to the initial REGISTER request with a valid 401 Unauthorized response.
3) The SS waits for the UE to set up a temporary set of security associations and to send another REGISTER request, over those security associations.
4) The SS responds to the second REGISTER request with valid 200 OK response, sent over the same temporary set of security associations that the UE used for sending the REGISTER request.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	The UE sends initial IMS emergency registration
2	←		401 Unauthorized	The SS responds with a valid AKAv1-MD5 authentication challenge and security mechanisms supported by the network.
3	→		REGISTER	The UE completes the security negotiation procedures, sets up a temporary set of SAs and uses those for sending another REGISTER with AKAv1-MD5 credentials.
4	←		200 OK	The SS responds with 200 OK.

NOTE: The default message contents in annex A are used with the following exceptions:

Specific Message Contents:

REGISTER (Step 1)

Use the default message 'REGISTER' in annex A.1.1 with condition A1 "Initial unprotected REGISTER" and condition A7 'Initial IMS emergency registration' simultaneously applying.

The contents of From and To headers of the REGISTER request shall be according to condition A7.401 Unauthorized for REGISTER (Step 4).

Use the default message '401 Unauthorized for REGISTER' in annex A.1.2.

REGISTER (Step 3)

Use the default message 'REGISTER' in annex A.1.1 with condition A2 "Subsequent REGISTER sent over security associations" and condition A7 'Initial IMS emergency registration' simultaneously applying.

The contents of From and To headers of the REGISTER request shall be according to condition A7.

200 OK for REGISTER (Step 4)

Use the default message '200 OK for REGISTER' in annex A.1.3 with condition A3 'Response for an emergency registration'.

C.21 Generic test procedure for setting up MTSI MO speech call for EPS

Test procedure:

1) MO speech is initiated on the UE. The call is initiated towards the URI configured to SS as px_CalleeUri Depending on the UE support this URI may be either SIP or Tel URI, possibly containing a dialstring indicating a global, home local or geo-local telephone number. SS waits the UE to send an INVITE request with first SDP offer

2) UE sends an INVITE request to the SS.

3) SS responds to the INVITE request with a 100 Trying response.

4) SS responds to the INVITE request with a 183 Session Progress response

5) SS waits for the UE to send a PRACK request possibly containing the second SDP offer.

6) SS responds to the PRACK request with a 200 OK.

7) SS waits for the UE to send a UPDATE request containing the final SDP offer.

8) SS responds to the UPDATE request with a 200 OK.

9) SS responds to the INVITE request with a 180 Ringing.

10) SS waits for the UE to send a PRACK request.

11) SS responds to the PRACK request with a 200 OK.

12) SS responds to the INVITE request with a 200 OK.

13) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE attempt an IMS speech call	
2	→		INVITE	UE sends INVITE with the first SDP offer.
3	←		100 Trying	SS sends a 100 Trying provisional response.
4	←		183 Session Progress	SS sends an SDP answer.
5	→		PRACK	UE acknowledges and optionally offer a second SDP if a dedicated EPS bearer is established by the network.
6	←		200 OK	SS sends a 200 OK and answers the second SDP if present.
7	→		UPDATE	Optional step: UE sends a second SDP if a dedicated EPS bearer is established by the network.
8	←		200 OK	Optional step: SS sends a 200 OK.
9	←		180 Ringing	SS sends a 180 Ringing.
10	→		PRACK	UE acknowledges.
11	←		200 OK	SS responds PRACK with 200 OK.
12	←		200 OK	SS responds INVITE with 200 OK.
13	→		ACK	UE acknowledges.

Specific Message Contents

INVITE (Step 2)

Use the default message 'INVITE for MO Call' in annex A.2.1 with the following exceptions:

Header/param	Value/Remark
Supported	
option-tag	*precondition*

Message-body	The following SDP types and values. Session description: - *v=0* - *o=*-(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s=*(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t=* (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:0* [Note 6] - *b=RR:0* [Note 6] - *b=RS:* (bandwidth-value) [Note 7] - *b=RR:* (bandwidth-value) [Note 7] Attributes for media: - *a=tcap:1 RTP/AVPF* [Note 2] - *a=pcfg:1 t=1* [Note 2] - *a=rtpmap: (payload type) AMR/8000* [Note 8] - *a=fmtp: (format) mode-change-capability=2; max-red=220* - *a=rtpmap: (payload type) telephone-event* [Note 5] - *a=ecn-capable-rtp: leap; ect=0* [Note 3] - *a=rtcp-fb:* nack ecn* [Note 3] - *a=rtcp-xr:ecn-sum* [Note 3] - *a=rtcp-rsize* [Note 3] - *a=ptime:20* - *a=maxptime:240* - *a=inactive* Attributes for media security mechanism: - *a=3ge2ae: requested* [Note 4] - *a=a=crypto:1 AES_CM_128_HMAC_SHA1_80inline:WVNfX19zZW1jdGwgKCkgewkyMjA7fQp9CnVubGVz|2^20|1:4FEC_* [Note 4] Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: A Release 9 or later UE offer AVPF. Note 3: Attributes for ECN Capability may be present if the UE supports Explicit Congestion Notification. Note 4: Attributes for media plane security are present if the use of end-to-access-edge security is supported b Note 5: a rate may be added to the 'telephone-event' seperated by '/' (e.g. 'telephone-event/8000') Note 6: This line shall be present if A.12/nn 3GPP TS 34.229-2 [5] is 'x'. Note 7: This line shall be present if A.12/nn 3GPP TS 34.229-2 [5] is 'm'. The RR value must be greater than 0 any value. Note 8: The AMR channel number shall be '/1' or omitted.

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/Remark
Supported option-tag	*precondition*
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for UE) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1, 4] - *b=AS:30* - *b=RS:* (bandwidth-value) [Note 5] - *b=RR:* (bandwidth-value) [Note 5] Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000/1* [Note 1] - *a=fmtp:* (format) mode-change-capability=2; max-red=220 [Note 1] - *a=ecn-capable-rtp: leap; ect=0* [Note 2] - *a=rtcp-fb:* nack ecn* [Note 2] - *a=rtcp-xr:ecn-sum* [Note 2] - *a=ptime:20* - *a=maxptime:240* Attributes for media security mechanism: - *a=3ge2ae: requested* [Note 1] - *a=crypto:1 AES_CM_128_HMAC_SHA1_80inline:PS1uQCVeeCFCanVmcjkpPywjNWhcYD0mXXtxaVBR|2^20|1:4* [Note 3] Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Note 1: The value for fmt, payload type (AMR) and format is copied from step 2. Note 2: Attributes for ECN Capability are present if the UE supports Explicit Congestion Notification. Note 3: Attributes for media plane security are present if the use of end-to-access-edge security is supported by UE. Note 4: transport port is the port number of the SS (see RFC 3264 clause 6). Note 5: The bandwidth-value is copied from step 2.

PRACK (Step 5)

Use the default message 'PRACK' in annex A.2.4 with the following exceptions:

Header/param	Value/Remark
Message-body	Header optional Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o=-* (username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) [Note 2] - *s=*(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 3] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000* [Note 3] [Note 5] - *a=fmtp:* (format) [Note 3, 4] - *a= sendrecv* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The sess-version shall been increased. Note 3: The value for fmt, payload type and format is not checked Note 4: Parameters for the AMR codec are not checked Note 5: The AMR channel number shall be '/1' or omitted.

200 OK for PRACK (Step 6)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	Header present if Prack (step 5) contained SDP. Contents if present: SDP body of the 200 response copied from the received PRACK and modified as follows: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; Attributes for preconditions: - *a=curr:qos remote sendrecv*

UPDATE (Step 7)

Use the default message 'UPDATE' in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Message-body	Same contents as specified in step 5.

200 OK for UPDATE (Step 8)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	SDP body of the 200 response copied from the received UPDATE and modified as follows: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; Attributes for preconditions: - *a=curr:qos remote sendrecv*

180 Ringing (Step 9)

Use the default message '180 Ringing for INVITE' in annex A.2.6 applying condition A3 (Response sent reliably).

C.22 Generic test procedure for setting up emergency speech call

Test procedure:

1) SS waits for UE to send an INVITE request.
2) The SS responds to the INVITE request with a 100 Trying response.
3) SS responds to the INVITE request with a 180 Ringing.
4) The SS responds to the INVITE request with a 200 OK.
5) The SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1	→		INVITE	UE sends INVITE with the first SDP offer.
2	←		100 Trying	SS sends a 100 Trying provisional response.
3	←		180 Ringing	SS sends a 180 Ringing.
4	←		200 OK	SS responds INVITE with 200 OK.
5	→		ACK	UE acknowledges.

Specific Message Contents

INVITE (Step 1)

Use the default message 'INVITE for MO Call' in annex A.2.1 with the following exceptions:

Header/param	Value/remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o*=(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s*=(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] Time description: - *t*= (start-time) (stop-time) Media description: - *m=audio* (transport port) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Note 1: At least one "c=" field shall be present. Note 2: AMR codec shall be present: there shall be at least one media format (fmt) with an rtpmap attribute for any AMR codec (i.e. matching 'AMR/*' or 'AMR-WB/*')

180 Ringing for INVITE (Step 3)

Use the default message '180 Ringing for INVITE' in annex A.2.6 with condition A4 '180 sent by the SS when setting up an emergency call'.

200 OK for INVITE (Step 4)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with condition A6 'Response sent by SS for INVITE for emergency call' and the following exceptions:

Header/param	Value/remark
Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1] - *b=AS:30* - *b=RS:0* - *b=RR:0* Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000* [Note 1] [Note2] - *a=fmtp:* (format) *mode-change-capability=2; max-red=220* - *a=ptime:20* *a=maxptime:240* Note 1: The value for fmt, payload type and format is copied from step 1. Note 2: The AMR channel number shall be '/1' or omitted.

C.23 Procedure to register another IMPU over existing SAs

The generic test procedure:

1 The UE initiates IMS registration for the new IMPU. SS waits for the UE to send an initial REGISTER request over the existing set of IPSec SAs.

2 The SS responds to the initial REGISTER request with a valid 401 Unauthorized response.

3 The SS waits for the UE to send another REGISTER request, over the existing security associations.

4 The SS responds to the second REGISTER request with valid 200 OK response

5 The SS sends a NOTIFY request for the registration event package.

6 The SS waits for the UE to respond to the NOTIFY with a 200 OK response.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	The UE sends initial registration for the new IMPU over the existing IPSec SAs
2	←		401 Unauthorized	The SS responds with a valid AKAv1-MD5 authentication challenge
3	→		REGISTER	The UE sends another REGISTER with AKAv1-MD5 credentials.
4	←		200 OK	The SS responds with 200 OK.
5	←		NOTIFY	The SS sends a NOTIFY for registration event package, containing partial registration state information for the newly registered public user identity in the XML body
6	→		200 OK	The UE responds with 200 OK.

NOTE: The default message contents in annex A are used apart from the XML body in step 5. The body shall be specified within the test case referring to this procedure.

C.24 Generic test procedure for SRVCC media removal

Test procedure:

1) UE sends an re-INVITE request to the SS.

2) SS responds to the INVITE request with a 100 Trying response.

3) SS responds to the INVITE request with a 200 OK.

4) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1	→		INVITE	UE sends INVITE with audio removed.
2	←		100 Trying	SS sends a 100 Trying provisional response.
3	←		200 OK	SS responds INVITE with 200 OK.
4	→		ACK	UE acknowledges.

Specific Message Contents

INVITE (Step 1)

Use the default message 'INVITE for MO Call' in annex A.2.1 with condition A5 (re-INVITE within a dialog) and the following exceptions:

Header/param	Value/Remark
Message-body	The following SDP types and values. Session description: - v=0 - o=-(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - s=(session name) - c=IN (addrtype) (connection-address for UE) [Note 1] - b=AS: (bandwidth-value) Time description: - t= (start-time) (stop-time) Media description: - m=audio 0 RTP/AVP (fmt) - c=IN (addrtype) (connection-address for UE) [Note 1] - b=AS: (bandwidth-value) - b=RS:0 - b=RR:0 Note 1: At least one "c=" field shall be present.

C.25 Generic test procedure for setting up MTSI MO video call for EPS

Test procedure:

1) MO video call is initiated on the UE. The call is initiated towards the URI configured to SS as px_CalleeUri Depending on the UE support this URI may be either SIP or Tel URI, possibly containing a dialstring indicating a global, home local or geo-local telephone number. SS waits the UE to send an INVITE request with first SDP offer

2) UE sends an INVITE request to the SS.

3) SS responds to the INVITE request with a 100 Trying response.

4) SS responds to the INVITE request with a 183 Session Progress response

5) SS waits for the UE to send a PRACK request possibly containing the second SDP offer.

6) SS responds to the PRACK request with a 200 OK.

7) SS waits for the UE to send a UPDATE request containing the final SDP offer.

8) SS responds to the UPDATE request with a 200 OK.

9) SS responds to the INVITE request with a 180 Ringing.

10) SS waits for the UE to send a PRACK request.

11) SS responds to the PRACK request with a 200 OK.

12) SS responds to the INVITE request with a 200 OK.

13) SS waits for the UE to send an ACK to acknowledge receipt of the 200 OK for INVITE.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1			Make the UE attempt an IMS video call	
2	→		INVITE	UE sends INVITE with the first SDP offer.
3	←		100 Trying	SS sends a 100 Trying provisional response.
4	←		183 Session Progress	SS sends an SDP answer.
5	→		PRACK	UE acknowledges and optionally offer a second SDP if a dedicated EPS bearer is established by the network.
6	←		200 OK	SS sends a 200 OK and answers the second SDP if present.
7	→		UPDATE	Optional step: UE sends a second SDP if a dedicated EPS bearer is established by the network.
8	←		200 OK	Optional step: SS sends a 200 OK.
9	←		180 Ringing	SS sends a 180 Ringing.
10	→		PRACK	UE acknowledges.
11	←		200 OK	SS responds PRACK with 200 OK.
12	←		200 OK	SS responds INVITE with 200 OK.
13	→		ACK	UE acknowledges.

Specific Message Contents

INVITE (Step 2)

Use the default message 'INVITE for MO Call' in annex A.2.1 with the following exceptions:

Header/param	Value/Remark
Supported	
option-tag	*precondition*

Message-body	The following SDP types and values. Session description: - *v=0* - *o=*(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) - *s=*(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS*: (bandwidth-value) Time description: - *t=* (start-time) (stop-time) Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000* [Note 3] - *a=fmtp:* (format) *mode-change-capability=2; max-red=220* - *a=rtpmap:* (payload type) *telephone-event* - *a=ptime:20* - *a=maxptime:240* - *a=inactive* Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Media description: - *m=video (transport port) RTP/AVPF* (fmt) or RTP/AVP (fmt) [Note 2] - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=tcap:1 RTP/AVPF* [Note 2] - *a=pcfg:1 t=1* [Note 2] - *a=rtpmap: (payload type) H264/90000* - *a=fmtp: (format) profile-level-id=42e00c; sprop-parameter \ sets=J0LgDJWgUH6Af1A=,KM46gA==* - *a=inactive*

	Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The tcap/pcfg attributes are present if RTP/AVP is present on the m line. Note 3: The AMR channel number shall be '/1' or omitted.

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	Value/Remark
Supported	
option-tag	*precondition*

Message-body	The following SDP types and values. Session description: - *v=0* - *o=1111111111 1111111111 IN* (addrtype) (unicast-address for UE) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio (transport port) RTP/AVP* (fmt) [Note 1] - *b=AS:* (bandwidth-value) [Note 1] - *b=RS:* (bandwidth-value) [Note 1] - *b=RR:* (bandwidth-value) [Note 1] Attributes for media: - *a=rtpmap:* (payload type) AMR/8000/1 [Note 1] - *a=fmtp:* (format) mode-change-capability=2; max-red=220 [Note 1] - *a=ptime:20* - *a=maxptime:240* Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Media description: - *m=video (transport port) RTP/AVPF* (fmt) [Note 1] - *b=AS:* (bandwidth-value) [Note 1] - *b=RS:* (bandwidth-value) [Note 1] - *b=RR:* (bandwidth-value) [Note 1] Attributes for media: - *a=acfg:1 t=1* [Note 2] - *a=rtpmap: (payload type)* [Note 1] - *a=fmtp: (format)* [Note 1] Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv*

	Note 1: The value for fmt, bandwidth, payload type and format copied from step 2 Note 2: Present if tcap/pcfg attributes were included in step 2.

PRACK (Step 5)

Use the default message 'PRACK' in annex A.2.4 with the exceptions:

Header/param	Value/Remark

Message-body	Header optional Contents if present: The following SDP types and values shall be present. Session description: - *v=0* - *o=*(username) (sess-id) (sess-version) IN (addrtype) (unicast-address for UE) [Note 2] - *s=*(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio (transport port) RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap:* (payload type) *AMR/8000* [Note 3] - *a=fmtp:* (format) - *a=sendrecv* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Media description: - *m=video (transport port) RTP/AVPF* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap: (payload type) H264/90000* - *a=fmtp: (format) profile-level-id=42e00c; sprop-parameter \ sets=J0LgDJWgUH6Af1A=,KM46gA==* - *a=sendrecv*

	Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: The sess-version shall been increased. Note 3: The AMR channel number shall be '/1' or omitted.

200 OK for PRACK (Step 6)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	**Value/remark**
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	Header present if Prack (step 5) contained SDP. Contents if present: SDP body of the 200 response copied from the received PRACK and modified as follows: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; Attributes for preconditions: - *a=curr:qos remote sendrecv*

UPDATE (Step 7)

Use the default message 'UPDATE' in annex A.2.5 with the following exceptions:

Header/param	**Value/remark**
Message-body	Same contents as specified in step 5.

200 OK for UPDATE (Step 8)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header optional Contents if present: *application/sdp*
Content-Length Value	Contents if header Content-Type is present: length of message-body
Message-body	SDP body of the 200 response copied from the received UPDATE and modified as follows: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; Attributes for preconditions: *- a=curr:qos remote sendrecv*

C.26 Generic test procedure for setting up MTSI MT video call for EPS

Test procedure

1) SS sends an INVITE request to the UE.
2) Void
3) SS may receive 100 Trying from the UE.
4) SS expects and receives 183 Session Progress from the UE.
5) SS sends PRACK to the UE to acknowledge the 183 Session Progress.
6) SS expects and receives 200 OK for PRACK from the UE.
7) SS sends UPDATE to the UE, with SDP indicating that precondition is met on the server side.
8) SS expects and receives 200 OK for UPDATE from the UE, with proper SDP as answer.
9) SS may receive 180 Ringing from the UE.
10) SS may send PRACK to the UE to acknowledge the 180 Ringing.
11) SS may receive 200 OK for PRACK from the UE.

11A) The UE accepts the session invite.

12) SS expects and receives 200 OK for INVITE from the UE.
13) SS sends ACK to the UE.
14) SS sends BYE to the UE.
15) SS expects and receives 200 OK for BYE from the UE.

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with the first SDP offer.
2				Void
3	→		100 Trying	(Optional) The UE responds with a 100 Trying provisional response
4	→		183 Session Progress	The UE sends 183 response reliably with the SDP answer to the offer in INVITE
5	←		PRACK	SS acknowledges the receipt of 183 response from the UE.
6	→		200 OK	The UE responds to PRACK with 200 OK.
7	←		UPDATE	SS sends an UPDATE with SDP offer indicating SS reserved resources.
8	→		200 OK	The UE acknowledges the UPDATE with 200 OK and includes SDP answer to acknowledge its current precondition status.
9	→		180 Ringing	(Optional) The UE responds to INVITE with 180 Ringing.
10	←		PRACK	(Optional) SS shall send PRACK only if the 180 response contains 100rel option tag within the Require header.
11	→		200 OK	(Optional) The UE acknowledges the PRACK with 200 OK.
11A				Make UE accept the video offer.
12	→		200 OK	The UE responds to INVITE with a 200 OK final response after the user answers the call.
13	←		ACK	The SS acknowledges the receipt of 200 OK for INVITE.
14	←		BYE	The SS sends BYE to release the call.
15	→		200 OK	The UE sends 200 OK for the BYE request and ends the call.

NOTE: The default messages contents in annex A are used with condition 'IMS security' or 'early IMS security' when applicable

Specific Message Content

INVITE (Step 1)

Use the default message 'INVITE for MT Call' in annex A.2.9 with the following exceptions:

Header/param	Value/remark
Supported	
option-tag	*precondition*

Message-body	The following SDP types and values. Session description: - *v=0* - *o=- 1111111111 1111111111 IN* (addrtype) (unicast-address for SS) - *s=IMS conformance test* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:30* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP 97* - *b=AS:30* - *b=RS:0* - *b=RR:2000* Attributes for preconditions: - *a=curr:qos local none* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos optional remote sendrecv* Attributes for media: - *a=rtpmap:97 AMR/8000/1* - *a=fmtp:97 mode-change-capability=2; max-red=220* - *a=ptime:20* - *a=maxptime:240* Media description: - *m=video (transport port) RTP/AVPF 98* - *b=AS: 315* - *b=RS: 0* - *b=RR: 2500* Attributes for media: - *a=rtpmap: 98 H264/90000* - *a=fmtp: 98 packetization-mode=0;profile-level-id=42e00c; * *sprop-parameter-sets=J0LgDJWgUH6Af1A=,KM46gA==* - *a=rtcp-fb:* trr-int 5000* - *a=rtcp-fb:* nack* - *a=rtcp-fb:* nack pli* - *a=rtcp-fb:* ccm fir* - *a=rtcp-fb:* ccm tmmbr*

	Attributes for preconditions: *- a=curr:qos local none* *- a=curr:qos remote none* *- a=des:qos mandatory local sendrecv* *- a=des:qos optional remote sendrecv*

100 Trying (Step 3)

Use the default message "100 Trying for INVITE" in annex A.2.2.

183 Session Progress (Step 4)

Use the default message "183 Session Progress" in annex A.2.3 with the following exceptions:

Header/param	**Value/remark**
Status-Line	
Reason-Phrase	Not checked
Require	
option-tag	*precondition*

Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o=*(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=*(username) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for preconditions: - *a=curr:qos local none* or *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv* Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 2] - *a=fmtp:*(format) Media description: - *m=video (transport port) RTP/AVPF* (fmt) - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap: 98 H264/90000* - *a=fmtp: 98 packetization-mode=0;profile-level-id=42e00c; * *sprop-parameter-sets=J0LgDJWgUH6Af1A=,KM46gA==* Attributes for preconditions: - *a=curr:qos local none* or *a=curr:qos local sendrecv* - *a=curr:qos remote none* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* - *a=conf:qos remote sendrecv*

	Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be '/1' or omitted.

PRACK (step 5)

Use the default message "PRACK" in annex A.2.4. No content body is included in this PRACK message.

200 OK (Step 6)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

UPDATE (step 7)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Value/remark

Message-body	The following SDP types and values. Session description: *- v=0* *- o=- 1111111111 1111111112 IN* (addrtype) (unicast-address for SS) *- s=IMS conformance test* *- c=IN* (addrtype) (connection-address for SS) *- b=AS:30* Time description: *-t=0 0* Media description: *- m=audio* (transport port) *RTP/AVP 97* *- b=AS:30* *- b=RS:0* *- b=RR:2000* Attributes for media: *- a=rtpmap:97 AMR/8000/1* *- a=fmtp:97 mode-change-capability=2; max-red=220* *- a=ptime:20* *- a=maxptime:240* *- a=sendrecv* Attributes for preconditions: *- a=curr:qos local sendrecv* *- a=curr:qos remote none* or *curr:qos remote sendrecv* [Note 1] *- a=des:qos mandatory local sendrecv* *- a=des:qos mandatory remote sendrecv* Media description: *- m=video (transport port) RTP/AVPF 98* *- b=AS: 315* *- b=RS: 0* *- b=RR: 2500* Attributes for media: *- a=rtpmap: 98 H264/90000* *- a=fmtp: 98 packetization-mode=0;profile-level-id=42e00c; * *sprop-parameter-sets=J0LgDJWgUH6Af1A=,KM46gA==* *- a=rtcp-fb:* trr-int 5000* *- a=rtcp-fb:* nack* *- a=rtcp-fb:* nack pli* *- a=rtcp-fb:* ccm fir* *- a=rtcp-fb:* ccm tmmbr* *- a=sendrecv*

	Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote none* or *curr:qos remote sendrecv* [Note 1] - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Note 1: Use the value (none/sendrecv) received from 183 Session Progress and attribute a=curr:qos local.

200 OK (step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type	
media-type	*application/sdp*
Content-Length	
value	length of message-body

Message-body	The following SDP types and values shall be present. Session description: - *v=0* - *o=*(username) (sess-id) (sess-version) *IN* (addrtype) (unicast-address for UE) - *s=*(session name) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) - *c=IN* (addrtype) (connection-address for UE) [Note 1] - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv* Attributes for media: - *a=rtpmap:*(payload type) *AMR/8000* [Note 2] - *a=fmtp:*(format) - *a=sendrecv* Media description: - *m=video (transport port) RTP/AVPF* (fmt) - *b=AS:* (bandwidth-value) - *b=RS:* (bandwidth-value) - *b=RR:* (bandwidth-value) Attributes for media: - *a=rtpmap: 98 H264/90000* - *a=fmtp: 98 packetization-mode=0;profile-level-id=42e00c; * *sprop-parameter-sets=J0LgDJWgUH6Af1A=,KM46gA==* - *a=sendrecv* Attributes for preconditions: - *a=curr:qos local sendrecv* - *a=curr:qos remote sendrecv* - *a=des:qos mandatory local sendrecv* - *a=des:qos mandatory remote sendrecv*

	Note 1: At least one "c=" field shall be present. Note 2: The AMR channel number shall be '/1' or omitted.

180 Ringing (step 9)

Use the default message "180 Ringing for INVITE" in annex A.2.6

PRACK (step 10)

Use the default message "PRACK" in annex A.2.4. No content body is included in this PRACK message

200 OK (step 11)

Use the default message '200 OK for other requests than REGISTER or SUBSCRIBE' in annex A.3.1.

200 OK (step 12)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

ACK (step 13)

Use the default message "ACK" in annex A.2.7.

BYE (step 14)

Use the default message "BYE" in annex A.2.8.

200 OK (step 15)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1.

C.27 Generic test procedure for forked response of MTSI MO speech call

Test procedure:

1) SS responds to the INVITE request with a 183 Session Progress response.

NOTE: Steps 1 to 4 in annex C.21 are performed before this generic test procedure is initiated. This procedure may be performed in parallel with step 5 and later steps in annex C.21.

2) SS waits for the UE to send a PRACK request possibly containing the second SDP offer.

3) SS responds to the PRACK request with a 200 OK.

4) SS waits for the UE to send a UPDATE request containing the final SDP offer.

5) SS responds to the UPDATE request with a 200 OK.

6) SS responds to the INVITE request with a 180 Ringing.

7) SS waits for the UE to send a PRACK request.

8) SS responds to the PRACK request with a 200 OK.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1	←		183 Session Progress	SS sends an SDP answer.
2	→		PRACK	UE acknowledges and optionally offer a second SDP if a dedicated EPS bearer is established by the network.
3	←		200 OK	SS sends a 200 OK and answers the second SDP if present.
4	→		UPDATE	Optional step: UE sends a second SDP if a dedicated EPS bearer is established by the network.
5	←		200 OK	Optional step: SS sends a 200 OK.
6	←		180 Ringing	SS sends a 180 Ringing.
7	→		PRACK	UE acknowledges.
8	←		200 OK	SS responds PRACK with 200 OK.

Specific Message Contents

183 Session Progress (Step 1)

Use the "183 Session Progress (Step 4)" in annex C.21 with the following exceptions:

Header/param	Value/remark
To	
tag	different value from px_InviteToTag

PRACK (Step 2)

Use the "PRACK (Step 5)" in annex C.21 with the following exceptions:

Header/param	Value/remark
To	
tag	same value as used in step 1

200 OK for PRACK (Step 3)

Use the "200 OK for PRACK (Step 6)" in annex C.21 with the following exceptions:

Header/param	Value/remark
To	
tag	same value as used in step 1

UPDATE (Step 4)

Use the "UPDATE (Step 7)" in annex C.21 with the following exceptions:

Header/param	Value/remark
To	
tag	same value as used in step 1

200 OK for UPDATE (Step 5)

Use the "200 OK for UPDATE (Step 8)" in annex C.21 with the following exceptions:

Header/param	Value/remark
To	
tag	same value as used in step 1

180 Ringing (Step 6)

Use the default message "180 Ringing for INVITE" in annex A.2.6 with the following exceptions:

Header/param	Value/remark
To	
tag	same value as used in step 1

PRACK (Step 7)

Use the default message "PRACK" in annex A.2.4 with the following exceptions:

Header/param	Value/remark
To	
tag	same value as used in step 1

200 OK for PRACK (Step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
To	
tag	same value as used in step 1

C.28 Generic test procedure for SIP UPDATE after aSRVCC handover failure/cancelled

Test procedure:

1) SS waits for the UE to send a UPDATE request containing the SDP offer same as used in the existing dialog.

2) SS responds to the UPDATE request with a 200 OK.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1	→		UPDATE	UE sends UPDATE.
2	←		200 OK	SS sends a 200 OK.

Specific Message Contents

UPDATE (Step 1)

Use the default message "UPDATE" in annex A.2.5 with the following exceptions:

Header/param	Value/remark
Reason	
protocol	*SIP*
reason-params	*cause=487; text="handover cancelled"*, if this procedure is performed after aSRVCC handover cancelled. *cause=487; text="failure to transition to CS domain"*, if this procedure is performed after aSRVCC handover failure.
Message-body	Same contents as used before SRVCC handover.

200 OK for UPDATE (Step 2)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 with the following exceptions:

Header/param	Value/remark
Content-Type	
media-type	*application/sdp*
Content-Length	Contents if header Content-Type is present:
Value	length of message-body
Message-body	SDP body of the 200 response copied from the received UPDATE and modified as follows: - IP address on "o=" and "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; Attributes for preconditions: - *a=curr:qos remote sendrecv*

C.29 Generic test procedures for Supplementary Services

C.29.1 Procedures for activation and deactivation of Supplementary Services

Test procedure:

0a) Pre-configurations:

The UE is IMS registered before any activation or deactivation of Supplementary Services is triggered. This will ensure more deterministic UE behaviours.

The UE has established a 2nd PDN connectivity (XCAP APN) for IMS XCAP signalling. In case of EUTRA the generic procedure according to TS 36.508 clause 4.5A.14 [94] shall be applied. During this procedure the UE may request a DNS server address via NAS signalling and as parallel behaviour the UE may resolve IP address IP addresses for XCAP server and BSF via DNS (FFS).

0b) In case of GAA XCAP authentication (referred to TS 33.222 [121] and TS 24.109 [119]), SS gets configured as HTTP server at port 80 (to simulate BSF) and port 443 (HTTPS) and the UE is expected to do authentication at the BSF according to the generic test procedure of C.29.2
In all other cases the SS gets configured as HTTP server at port 80 (HTTP) only.

1) Activation of the specific Supplementary Service is triggered at the UE with appropriate MMI command.

2) The UE sends an initial HTTP request to the SS.

3) In case of HTTP Digest XCAP authentication when the UE does not provide correct authorization credentials within its initial request:

3a) the SS shall challenge the UE by sending a '401 Unauthorized' response to it.

3b) the UE repeats the HTTP request including a valid digest response in the authorization header. The SS shall check the digest response taking into account the user"s password being "xcap".

4) The SS sends a 200 (OK) response

5) Optionally UE and SS exchange a sequence of additional HTTP requests and responses. In this sequence the UE may query the contents of the simservs document or selected parts of it.
In general the HTTP requests are responded with a 200 'Ok' response but in case of a GET request to a non-existing node the SS shall respond with a 404 'File Not Found'.

6) The simservs document is checked according to specific test requirements.

7) Deactivation of supplementary service is triggered at the UE with appropriate MMI command.

8) UE and SS exchange a sequence of HTTP requests and responses. In this sequence the UE may query the contents of the simservs document or selected parts of it.
In general the HTTP requests are responded with a 200 'Ok' response but in case of a GET request to a non-existing node the SS shall respond with a 404 'File Not Found'.

9) The simservs document is checked according to specific test requirements.

Expected sequence:

Step	Direction		Message/Procedure	Comment
	UE	SS		
1			Make the UE attempt activation of supplementary service	
2	→		Initial HTTP Request	NOTE 1
3			EXCEPTION: steps 3a and 3b describe behaviour in case of HTTP Digest XCAP authentication when the UE does not provide correct authorization credentials within its initial request	
3a	←		HTTP Response: '401 Unauthorized'	
3b	→		HTTP Request with valid authorization credentials	The SS checks the digest response
4	←		HTTP Response: '200 OK'	
5			EXCEPTION: steps 5a and 5b describe further optional message exchange between the UE and the SS; steps 5a and steps 5b can be repeated several times this exchange of information is considered to be finished when there is no further HTTP request sent by the UE within 20 seconds after the previous request	
5a	→		HTTP Request	NOTE 1
5b	←		HTTP Response: '200 OK' or '404 File Not Found'	NOTE 3
6			Check: Does the simservs document stored in the SS contain the information supplied by the UE as required by the test requirements of the specific test case?	This is done by fetching the whole simservs document from the XCAP server and checking its content against the respective XML file (according to the XSD definitions for the respective supplementary service)
7			Make the UE attempt deactivation of supplementary service	
8			EXCEPTION: steps 8a and 8b describe the mandatory message exchange between the UE and the SS which can be repeated several times; this exchange of information is considered to be finished when there is no further HTTP request sent by the UE within 10 seconds after the previous request	
8a	→		HTTP Request	NOTE 1
8b	←		HTTP Response: '200 OK' or '404 File Not Found'	NOTE 3
9			Check: Does the simservs document stored in the SS contain the information supplied by the UE as required by the test requirements of the specific test case?	This is done by fetching the whole simservs document from the XCAP server and checking its content against the respective XML file (according to the XSD definitions for the respective supplementary service)
NOTE 1: The HTTP requests sent by the UE are processed by an XCAP server implementation at the SS to modify the contents of the simservs document. NOTE 2: Any other UL messages (HTTP Request) appearing in the test sequence are ignored. NOTE 3: '404 File Not Found' is sent as response for a GET request to a non-existing node				

Specific Message Contents

HTTP Requests sent by the UE (step 2, 3b, 5a, 8a)

Header/param	Value/remark	Rel	Reference
Request-Line			RFC 2616 [69]
Method	*GET, PUT, DELETE*		
Request-URI	XCAP URI referring to the simservs document as specified in RFC 4825 [70]; the document selector of such XCAP URI consists of - Configured XCAP root URI - *simservs.ngn.etsi.org* - *users* - Public user id as used for activation/deactivation of the supplementary service (NOTE 2) - *simservs.xml* (in this order, separated by a slash); According to RFC 4825 [70] the node selector of the XCAP URI shall identify a valid part of a simservs document or whole document itself (NOTE 3).		
Version	HTTP 1.1		
Authorization	present in case of HTTP Digest XCAP authentication in the initial request or in the request following the '401 Unauthorized' response		RFC 2617 [16] RFC 3310 [17]
username	private user identity as stored in EF_{IMPI} (when using ISIM) or private user identity derived from IMSI (when no ISIM available on the UICC)		
realm	same value as received in the realm directive in the WWW Authenticate header sent by SS		
nonce	same value as in WWW-Authenticate header sent by SS		
opaque	same value as sent by the SS in '401 Unauthorized'		
digest-uri	same URI as used in Request-URI		
qop-value	*auth*		
cnonce-value	value assigned by UE affecting the response calculation		
nonce-count	1		
response	response calculated by UE		
algorithm	*MD5*		
Content-Type	present for HTTP PUT method		RFC 2616 [69]
media-type	*application/vnd.etsi.simservs+xml* or *application/xcap-el+xml* or *application/xcap-att+xml* (NOTE 4)		
Message-body	present for HTTP PUT method: XML fragment of given node		RFC 2616 [69] RFC 4825 [70]

NOTE 1: Any other headers are ignored.
NOTE 2: As working assumption the UE gets a valid public user id (e.g. as stored on the ISIM) handed over with the MMI command corresponding to activation/deactivation of the supplementary service
NOTE 3: The SS shall check and make sure that the syntax of the node selector expressions is in compliance to clause 6.2 of RFC 4825 [70].
NOTE 4: the media-type depends on the kind of node being accessed by the Request-URI: document, element or attribute (see RFC 4825 [70]).

HTTP Responses (step 4, 5b, 8b2, 4) – normal case

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 2616 [69]
Version	HTTP 1.1		
Code	200		
Reason	OK		
Content-Type	present for HTTP GET method		RFC 2616 [69]
media-type	*application/vnd.etsi.simservs+xml* or *application/xcap-el+xml* or *application/xcap-att+xml* (NOTE 1)		
Message-body	present for GET method: XML fragment of given node		RFC 2616 [69] RFC 4825 [70]
NOTE 1: the media-type depends on the kind of node being accessed with the HTTP GET method: document, element or attribute (see RFC 4825 [70]).			

HTTP Responses (step 5b, 8b) – Response for GET request to a non-existing node

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 2616 [69]
Version	HTTP 1.1		
Code	404		
Reason	File Not Found		

HTTP Response (step 3a) for HTTP Digest XCAP authentication

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 2616 [69]
Version	HTTP 1.1		
Code	401		
Reason	Unauthorized		
WWW-Authenticate			RFC 2616 [69]
realm	home domain name as stored in EF_{DOMAIN} or home domain name derived from the IMSI		
algorithm	*MD5*		
qop-value	*auth*		
nonce	Base 64 encoding of RAND and AUTN		
opaque	arbitrary value (to be returned by the UE in subsequent REGISTER)		

C.29.2 Procedure for GAA XCAP authentication

Test procedure:

The generic test procedure for GAA XCAP authentication is referred to the bootstrapping procedure in TS 33.220 [120], clause 4.5.2.

Expected sequence:

Step	Direction		Message	Comment
	UE	SS		
1	→		HTTP Request	
2	←		HTTP Response: '401 Unauthorized'	
3	→		HTTP Request with valid authorization credentials	
4	←		HTTP Response: '200 OK'	
NOTE: Any other UL messages (HTTP Request) appearing in the test sequence are ignored.				

Specific Message Contents

HTTP Request (step 1)

Header/param	Value/remark	Rel	Reference
Request-Line			RFC 2616 [69]
Method	*FFS*		
Request-URI	*FFS*		
Version	HTTP 1.1		
NOTE: Any other headers are ignored.			

HTTP Response (step 2)

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 2616 [69]
Version	HTTP 1.1		
Code	401		
Reason	Unauthorized		
WWW-Authenticate			RFC 2616 [69]
realm	*FFS*		
algorithm	*FFS*		
qop-value	*FFS*		
nonce	*FFS*		
opaque	*FFS*		

HTTP Request (step 3)

Header/param	Value/remark	Rel	Reference
Request-Line			RFC 2616 [69]
Method	*FFS*		
Request-URI	*FFS*		
Version	HTTP 1.1		
Authorization			RFC 2616 [69]
username	*FFS*		
realm	*FFS*		
nonce	*FFS*		
opaque	*FFS*		
digest-uri	*FFS*		
qop-value	*FFS*		
cnonce-value	*FFS*		
nonce-count	*FFS*		
response	*FFS*		
algorithm	*FFS*		
NOTE: Any other headers are ignored.			

HTTP Response (step 4)

Header/param	Value/remark	Rel	Reference
Status-Line			RFC 2616 [69]
Version	HTTP 1.1		
Code	200		
Reason	OK		
Expires			RFC 2616 [69]
delta-seconds	*FFS*		

C.30 Generic test procedure for Mobile Initiated Deregistration

The generic test procedure:

1 The UE is triggered by MMI to initiate a deregistration procedure

2 IMS deregistration is initiated on the UE. SS waits for the UE sending a REGISTER request, in accordance with 3GPP TS 24.229 [10], clause 5.1.1.6

Expected sequence:

Step	Direction		Message/Procedure	Comment
	UE	SS		
1	→		REGISTER	The UE sends deregistration for IMS services
2	←		200 OK	The SS responds to REGISTER with 200 OK
-	-		EXCEPTION: the next step is performed only if a TCP connection is used for IMS signalling.	
3	-		The SS waits for [3] s.	Delay is added to ensure that UE closes down the TCP connection after the IMS deregistration procedure before proceeding with other signalling procedures.

Specific message contents

REGISTER (step 1)

Use the default message 'REGISTER' in annex A.1.1 with condition A2 or A3 in accordance to 3GPP TS 24.229 [10] clause 5.1.1.6 with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	SIP URI with IP address or FQDN and protected server port of UE or *
expires	*0* (if present)
Expires	(must be present if addr-spec is *)
delta-seconds	*0* (if present)
Supported	header may be missing or it may contain any value
Authorization	
nonce-count	value not checked

200 OK (step 2)

Use the default message '200 OK for REGISTER' in annex A.1.3 with the following exceptions:

Header/param	Value/remark
Contact	
addr-spec	*same value as in REGISTER request if "*" is not included in the Contact header field of the REGISTER request in step 1* *same value as in the Contact header field of the "200 OK" response to the initial registration if "*" is included in the Contact header field of the REGISTER request in step 1 (NOTE)*
expires	*0*
NOTE: According to 3GPP TS 24.229 [10] clause 5.4.1.4.1 when the S-CSCF gets a wild-carded contact address for de-registration it shall include all de-registered contact addresses in the contact header of the 200 OK response ⇒ there is no '*' in DL.	

Annex D (Informative): Example values for certain IXIT parameters

This table contains syntactically correct example values for a number of headers and parameters that may be used as such by SS when sending downlink messages and checking that the uplink messages would contain the same values. These values will be defined as IXIT.

IMS registration parameters from ISIM application			
px_HomeDomainName	3gpp.org		
px_PublicUserIdentity	sip:localuser@3gpp.org		
px_PrivateUserIdentity	privateuser@3gpp.org		
IMS registration parameters derived from IMSI when using USIM application			TS 23.003 [32]
px_IMSI	12345611223344		
home domain name	ims.mnc123.mcc456.3gppnetwork.org		
public user identity	sip:12345611223344@ ims.mnc123.mcc456.3gppnetwork.org		
private user identity	12345611223344@ ims.mnc123.mcc456.3gppnetwork.org		
CSCF domain names			
px_pcscf	pcscf.3gpp.org	(FQDN that resolves to the IP address of SS)	
px_scscf	scscf.3gpp.org	(FQDN that does not resolve to the IP address of SS)	

Annex E (normative): Test ISIM Parameters

E.1 Introduction

This annex defines the default parameters to be programmed into the elementary files of the ISIM application.

Access conditions, data items and coding for the EFs for IMS session are defined in clause 4 of 3GPP TS 31.103 [31.103].

The parameters to be programmed into the elementary files for the USIM application are defined in clause 8.3 of 3GPP TS 34.108 [34.108].

E.2 Definitions

"Test ISIM card":

A ISIM card supporting the test algorithm for authentication defined in clause 8.1.2 of [34.108], programmed with the parameters defined in this annex and clause 8 of 3GPP TS 34.108 [34.108].

E.3 Default settings for the Elementary Files (EFs)

The format and coding of elementary files of the ISIM/USIM are defined in 3GPP TS 31.101 [31.101] and 3GPP TS 31.103 [31.103].

This annex defines the default parameters to be programmed into each elementary file of the ISIM/USIM.

If EFs have an unassigned value, it may not be clear from the main text what this value should be. This annex suggests values in these cases.

E.3.1 Contents of the EFs at the MF level

The contents of the EFs at the MF level is defined in clause 8.3.1 in 3GPP TS 34.108 [34.108].

E.3.2 Contents of files at the ISIM ADF (Application DF) level

E.3.2.1 EF_{IMPI} (IMS private user identity)

As defined in TS 31.121 [113].

E.3.2.2 EF_{DOMAIN} (Home Network Domain Name)

As defined in TS 31.121 [113].

E.3.2.3 EF_{IMPU} (IMS public user identity)

As defined in TS 31.121 [113], but with MCC and MNC values aligned to the HPLMN of the EF IMSI in the USIM ADF according to clause 8.3.2.2 in 3GPP TS 34.108 [40].

E.3.2.4 EF_{AD} (Administrative Data)

This EF is programmed as defined in clause 8.3.2.18 in 3GPP TS 34.108 [40].

E.3.2.5 EF_{ARR} (Access Rule Reference)

The programming of this EF is a test house option.

E.3.2.6 EF_{IST} (ISIM Service Table)

As defined in TS 31.121 [113].

E.3.2.7 $EF_{P\text{-}CSCF}$ (P-CSCF Address)

As defined in TS 31.121 [113].

E.3.2.8 EF_{GBABP} (GBA Bootstrapping parameters)

The programming of this EF is a test house option.

E.3.2.9 EF_{GBANL} (GBA NAF List)

The programming of this EF is a test house option.

E.3.2.10 EF_{NAFKCA} (NAF Key Centre Address)

The programming of this EF is a test house option.

E.3.2.11 EF_{SMS} (Short messages)

As defined in TS 31.121 [113].

E.3.2.12 EF_{SMSS} (SMS status)

As defined in TS 31.121 [113].

E.3.2.13 EF_{SMSR} (Short message status reports)

As defined in TS 31.121 [113].

E.3.2.14 EF_{SMSP} (Short message service parameters) As defined in TS 31.121 [113].

E.3.2.15 $EF_{PSISMSC}$ (Public Service Identity of the SM-SC)

As defined in TS 31.121 [113].

This EF must be present on the ISIM if ISIM is used or on the USIM if USIM is used.

Annex F (normative): Generic Requirements for MTSI Supplementary Services

This Annex contains references to such generic requirements for IMS Multimedia Telephony Supplementary Services which apply to multiple test cases. These references are to the 3GPP documents, most of which were earlier annexes of TS 24.173 [65].

F.1 XCAP over Ut interface

The generic UE requirements for XCAP over Ut interface are specified in 3GPP TS 24.623 [105] clauses 4, 5.1, 5.2.1, 5.3.1 and 6.

NOTE: 3GPP TS 24.173 refers to this document as its Annex I.

The generic UE requirements for XCAP authentication over Ut interface are specified in 3GPP 24.623 [105] clause 5.2.1.1 and TS 33.220 clauses 4 and 4.3.1

[TS 24.623 clause 5.2.1.1]:

For systems where Generic Authentication Architecture is used, the UE shall support the authentication mechanisms specified in 3GPP TS 33.222 and 3GPP TS 24.109.

For systems where Generic Authentication Architecture is not used, the UE shall support RFC 2617 and RFC 2246 according to ETSI TS 183 038.

…

[TS 33.220 clause 4]:

The 3GPP authentication infrastructure, including the 3GPP Authentication Centre (AuC), the USIM or the ISIM, and the 3GPP AKA protocol run between them, is a very valuable asset of 3GPP operators. It has been recognised that this infrastructure could be leveraged to enable application functions in the network and on the user side to establish shared keys. Therefore, 3GPP can provide the "bootstrapping of application security" to authenticate the subscriber by defining a Generic Bootstrapping Architecture (GBA) based on AKA protocol.

…

[TS 33.220 clause 4.3.1]:

The reference point Ub is between the UE and the BSF. Reference point Ub provides mutual authentication between the UE and the BSF. It allows the UE to bootstrap the session keys based on 3GPP AKA infrastructure.

The HTTP Digest AKA protocol, which is specified in RFC 3310, is used on the reference point Ub. It is based on the 3GPP AKA TS 33.102 protocol. The interface to the USIM is as specified in TS 31.102 and to the ISIM is as specified in TS 31.103.

F.2 Originating Identification Presentation (OIP) / Originating Identification Restriction (OIR)

The UE requirements for Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR) are specified in 3GPP TS 24.607 [102] clauses 4.2, 4.5.0, 4.5.1, 4.5.2.1, 4.5.2.12 and 4.10.

NOTE: 3GPP TS 24.173 refers to this document as its Annex A.

F.3 Terminating Identification Presentation (TIP) / Terminating Identification Restriction (TIR)

The UE requirements for Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR) are specified in 3GPP TS 24.608 [103] clauses 4.2, 4.5.0, 4.5.1, 4.5.2.1, 4.5.2.12 and 4.9.

NOTE: 3GPP TS 24.173 refers to this document as its Annex B.

F.4 Communication Diversion (CDIV)

The UE requirements for Communication Diversion (CDIV) are specified in 3GPP TS 24.604 [106] clauses 4.2, 4.5.0, 4.5.1, 4.5.2.1, 4.5.2.15, 4.5.2.16 and 4.9.

NOTE: 3GPP TS 24.173 refers to this document as its Annex C.

F.5 Communication Barring (CB)

The UE requirements for Communication Barring (CB) are specified in 3GPP TS 24.611 [101] clauses 4.2, 4.5.0, 4.5.1, 4.5.2.1, 4.5.2.13 and 4.9.

NOTE: 3GPP TS 24.173 refers to this document as its Annex E.

Annex G (informative): Change history

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-31	RP-060052	-	-	Update to version 1.0.0 and present to RAN#31 for information	-	0.0.1	1.0.0	R5-060292
-	-	-	-	Update to version 2.0.0 at RAN5#31	-	1.0.0	2.0.0	R5-061398
-	-	-	-	Update to version 2.1.0 during RAN5#31 e-mail agreement procedure	-	2.0.0	2.1.0	R5-061398r1
RP-32	RP-060269	-	-	MCC Editorial clean up version 2.1.1 - and present to RAN#32 for approval to go under revision control (as version 5.0.0)	-	2.1.0	2.1.1	-
-	-	-	-	Update to version 5.0.0 after RAN#32	-	2.1.1	5.0.0	-
RP-33	RP-060565	0001	-	Correction to TS 34.229-1 contents	F	5.0.0	5.1.0	R5-062360
RP-33	RP-060565	0002	-	Clarification to Emergency Test Case	F	5.0.0	5.1.0	R5-062543
RP-33	RP-060565	0003	-	Clarifications for SDP handling in TC 12.1 MO Call Successful	F	5.0.0	5.1.0	R5-062309
RP-33	RP-060565	0004	-	Test Case Correction on SigComp in the Initial registration	F	5.0.0	5.1.0	R5-062362
RP-33	RP-060565	0005	-	New TC on SigComp in the MO Call	F	5.0.0	5.1.0	R5-062323
RP-33	RP-060565	0006	-	Correction to authentication test case 9.2 Invalid Behaviour – SQN out of range	F	5.0.0	5.1.0	R5-062372
RP-33	RP-060565	0007	-	New TC on SigComp in the MT Call	F	5.0.0	5.1.0	R5-062363
RP-33	RP-060565	0008	-	New test cases for P-CSCF Discovery List	F	5.0.0	5.1.0	R5-062364
RP-33	RP-060565	0009	-	General IMS testing corrections and clarifications	F	5.0.0	5.1.0	R5-062371
RP-33	RP-060565	0010	-	Alignment with TS 24.229 version 5.16.0 affecting TCs 8.1, 8.2, 8.3 and the default message REGISTER.	F	5.0.0	5.1.0	R5-062215
RP-33	RP-060565	0011	-	Correction for TC 8.4: Invalid Behaviour – 423 Interval Too Brief	F	5.0.0	5.1.0	R5-062216
RP-33	RP-060565	0012	-	Correction for TCs 9.1and 9.2	F	5.0.0	5.1.0	R5-062370
RP-34	RP-060746	0013	-	Introduction of default messages and generic registration test procedure for early IMS security	F	5.1.0	5.2.0	R5-063332
RP-34	RP-060746	0014	-	Introduction of a registration test case for early IMS security	F	5.1.0	5.2.0	R5-063384
RP-34	RP-060746	0015	-	Updating of test cases to cover both IMS support and early IMS security scenarios	F	5.1.0	5.2.0	R5-063529
RP-34	RP-060746	0016	-	Introduction of a registration test case for combined IMS support and early IMS security	F	5.1.0	5.2.0	R5-063526
RP-34	RP-060746	0017	-	Introduction of a registration test case for combined IMS support and early IMS security and UICC with SIM application	F	5.1.0	5.2.0	R5-063385
RP-34	RP-060746	0018	-	Removal of MO Call - 488 not accepted here for Rel 5	F	5.1.0	5.2.0	R5-063330
RP-34	RP-060746	0019	-	Clarifications to MT test case	F	5.1.0	5.2.0	R5-063386
RP-34	RP-060746	0020	-	Corrections to MO with sigcomp test case	F	5.1.0	5.2.0	R5-063387
RP-34	RP-060746	0021	-	Corrections to P-CSCF Discovery (IPv6) test cases	F	5.1.0	5.2.0	R5-063388
RP-34	RP-060746	0022	-	New TCs on SigComp Invalid Behaviour	F	5.1.0	5.2.0	R5-063389
RP-34	RP-060746	0023	-	Addition of annex with the test ISIM parameters	F	5.1.0	5.2.0	R5-063390
RP-34	RP-060746	0024	-	Introduction of a postamble for IMS testing	F	5.1.0	5.2.0	R5-063391
RP-34	RP-060746	0025	-	Correction to Generic DHCP test procedure	F	5.1.0	5.2.0	R5-063242
RP-34	RP-060746	0027	-	Clarifications for IMS emergency call test case 14.2	F	5.1.0	5.2.0	R5-063522
RP-34	RP-060746	0028	-	Clarification of Default Message for IMS emergency call test case 14.2	F	5.1.0	5.2.0	R5-063523
RP-34	RP-060748	0033	-	Update of PDP Context and P-CSCF Discovery test cases to Rel-6	F	5.1.0	5.2.0	R5-063572
RP-34	RP-060746	0026	-	Production of pointer version 5.2.0 of TS 34.229-1 with no technical contents	F	5.1.0	5.2.0	R5-063291
RP-34	RP-060748	0029	-	Updates to TC 11.1 Network-initiated deregistration for IMS Rel-6	F	5.1.0	6.0.0	R5-063574
RP-34	RP-060748	0030	-	Updates to TC 11.2 Network initiated re-authentication for IMS Rel-6	F	5.1.0	6.0.0	R5-063573
RP-34	RP-060748	0031	-	Updates to TC 12.1 MO Call Successful for IMS Rel-6	F	5.1.0	6.0.0	R5-063570
RP-34	RP-060748	0032	-	Updates to TC 8.1 Initial registration for IMS Rel-6	F	5.1.0	6.0.0	R5-063569
RP-35	RP-070088	0034	-	New TC 12.6	F	6.0.0	6.1.0	R5-070408
RP-35	RP-070088	0035	-	New TC 12.7	F	6.0.0	6.1.0	R5-070447
RP-35	RP-070088	0036	-	New TC 12.8	F	6.0.0	6.1.0	R5-070446

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-35	RP-070088	0037	-	TC 8.5 Conformance requirement update	F	6.0.0	6.1.0	R5-070099
RP-35	RP-070088	0038	-	TC 8.6 Conformance requirement update	F	6.0.0	6.1.0	R5-070410
RP-35	RP-070088	0039	-	TC 8.7 Conformance requirement update	F	6.0.0	6.1.0	R5-070101
RP-35	RP-070088	0040	-	TC 12.2 Conformance requirement update	F	6.0.0	6.1.0	R5-070102
RP-35	RP-070088	0041	-	Corrections and updating default message according release 6	F	6.0.0	6.1.0	R5-070407
RP-35	RP-070088	0042	-	IMS security and early IMS security capability update	F	6.0.0	6.1.0	R5-070104
RP-35	RP-070088	0043	-	Correct missing IMS security in TC 14.2	F	6.0.0	6.1.0	R5-070105
RP-35	RP-070088	0044	-	Rename TC 8.6 and 8.7 to include 'IMS security' instead of 'IMS support'	F	6.0.0	6.1.0	R5-070106
RP-35	RP-070088	0045	-	Updates to 34.229 TC 12.1	F	6.0.0	6.1.0	R5-070412
RP-35	RP-070088	0046	-	Corrections to P-CSCF Discovery (IPv4) test cases	F	6.0.0	6.1.0	R5-070413
RP-35	RP-070088	0047	-	New IMS CC test case for MO call initiation when MO UE supports and uses preconditions whereas MT UE does not support preconditions (TC 12.5).	F	6.0.0	6.1.0	R5-070414
RP-35	RP-070088	0048	-	Updates to TC 8.2 User Initiated Re-Registration for IMS Rel-6	F	6.0.0	6.1.0	R5-070415
RP-35	RP-070088	0049	-	Removal of IMS CC test cases 7.7 and 7.8	F	6.0.0	6.1.0	R5-070210
RP-35	RP-070088	0050	-	Update IMS default message content for 503 Service Unavailable response	F	6.0.0	6.1.0	R5-070416
RP-35	RP-070088	0051	-	Update Specific message Content for 503 response in IMS TCs 10.1 and 12.2.	F	6.0.0	6.1.0	R5-070417
RP-35	RP-070088	0052	-	Updates to TC 13.1 SigComp in the Initial registration for IMS Rel-6	F	6.0.0	6.1.0	R5-070418
RP-35	RP-070088	0053	-	Updates to TC 13.2 SigComp in the MO Call for IMS Rel-6	F	6.0.0	6.1.0	R5-070419

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-35	RP-070089	0054	-	Updates to TC 13.3 SigComp in the MT Call for IMS Rel-6	F	6.0.0	6.1.0	R5-070420
RP-35	RP-070089	0055	-	Updates to TC 13.4 State creation before authentication for IMS Rel-6	F	6.0.0	6.1.0	R5-070421
RP-35	RP-070089	0056	-	Correction to test case 7.4	F	6.0.0	6.1.0	R5-070309
RP-35	RP-070089	0057	-	Rel-6 ISIM parameters	F	6.0.0	6.1.0	R5-070310
RP-35	RP-070089	0058	-	Updates to TC 12.4 Call initiation – Mobile termination for IMS Rel-6	F	6.0.0	6.1.0	R5-070424
RP-35	RP-070089	0059	-	Updates to TC 8.3 User initiated deregistration for IMS Rel-6	F	6.0.0	6.1.0	R5-070425
RP-36	RP-070362	0060	-	Usage of comp=sigcomp parameter in IMS TC 13.4	F	6.1.0	6.2.0	R5-071059
RP-36	RP-070362	0061	-	IMS TC 7.1: Additional option for coding the IPv4 address in PCO IE	F	6.1.0	6.2.0	R5-071437
RP-36	RP-070362	0062	-	Clarification on Require header in the UPDATE message for MT SigComp TC	F	6.1.0	6.2.0	R5-071489
RP-36	RP-070362	0063	-	Splitting MO Call TC 12.1 to Rel-5 and Rel-6 variants	F	6.1.0	6.2.0	R5-071496
RP-36	RP-070362	0064	-	Corrections and updates to TC 12.6	F	6.1.0	6.2.0	R5-071497
RP-36	RP-070362	0065	-	Corrections and updates to TC 12.7	F	6.1.0	6.2.0	R5-071498
RP-36	RP-070362	0066	-	Corrections and updates to TC 12.8	F	6.1.0	6.2.0	R5-071499
RP-36	RP-070362	0067	-	New TC MO Call (no resource reservation, preconditions used)	F	6.1.0	6.2.0	R5-071500
RP-36	RP-070362	0068	-	New TC MT Call (no resource reservation, preconditions used)	F	6.1.0	6.2.0	R5-071501
RP-36	RP-070362	0069	-	Clarification of test case purpose for TC 8.7 (wrong spec nr on the coversheet indicating 34.229-2, initially	F	6.1.0	6.2.0	R5-071488
RP-37	RP-070607	0070	-	Clarify parameter description in specific message contents	F	6.2.0	6.3.0	R5-072111
RP-37	RP-070607	0071	-	Update the SDP RFC reference	F	6.2.0	6.3.0	R5-072112
RP-37	RP-070607	0072	-	New TC User initiated re-registration for early IMS	F	6.2.0	6.3.0	R5-072113
RP-37	RP-070607	0073	-	Correction to IMS CC test case 12.4	F	6.2.0	6.3.0	R5-072119
RP-37	RP-070594	0074	-	Default message correction for 401 response	F	6.2.0	6.3.0	R5-072504
RP-37	RP-070594	0075	-	Correct check of ACK message in 12.9	F	6.2.0	6.3.0	R5-072508
RP-37	RP-070594	0076	-	Handling of optional PUBLISH messages	F	6.2.0	6.3.0	R5-072507
RP-37	RP-070607	0077	-	Correct the check of SDP answer to the SDP offer	F	6.2.0	6.3.0	R5-072511
RP-37	RP-070607	0078	-	Correct the re-invite message in 12.6	F	6.2.0	6.3.0	R5-072481
RP-37	RP-070594	0079	-	IMSCC Test 8.3 / Supported header in Register message for de-registration	F	6.2.0	6.3.0	R5-072505
RP-37	RP-070594	0080	-	Format of home domain name within the ISIM	F	6.2.0	6.3.0	R5-072506
RP-37	RP-070607	0081	-	New TC Mobile initiated de-registration for early IMS	F	6.2.0	6.3.0	R5-072495
RP-38	RP-070874	0087		IMS - Change of SUBSCRIBE Via header default value	F	6.3.0	6.4.0	R5-073468
RP-38	RP-070874	0086		Production of 34.229-1 pointer version in Rel-6 pointing to Rel-7 version	F	6.3.0	6.4.0	R5-073278
RP-38	RP-070882	0082		Updating references of 34.229-1 for MTSI and GRUU	F	6.3.0	7.0.0	R5-073036
RP-38	RP-070882	0083		Updating case 8.1 Initial Registration for 24.229 Rel-7	F	6.3.0	7.0.0	R5-073440
RP-38	RP-070882	0084		New IMS Rel-7 test case for MO MTSI voice call	F	6.3.0	7.0.0	R5-073298
RP-38	RP-070882	0085		New IMS Rel-7 test case for MO MTSI call hold	F	6.3.0	7.0.0	R5-073444
RP-39	RP-080113	0088		Centralizing rules for dialog identifiers to common messages	F	7.0.0	7.1.0	R5-080025
RP-39	RP-080113	0089		Updating conformance requirements of registration test cases for Rel-7	F	7.0.0	7.1.0	R5-080026
RP-39	RP-080113	0090		Updating references of 34.229-1 to IETF RFCs related to MTSI	F	7.0.0	7.1.0	R5-080368
RP-39	RP-080113	0091		New Annex F for generic requirements of MTSI supplementary services	F	7.0.0	7.1.0	R5-080598
RP-39	RP-080113	0092		Update of common messages for MTSI communication service identifier	F	7.0.0	7.1.0	R5-080029
RP-39	RP-080113	0093		New MTSI test case 15.12 MT call hold	F	7.0.0	7.1.0	R5-080485
RP-39	RP-080113	0094		New MTSI test case 15.13 Incoming Communication Barring	F	7.0.0	7.1.0	R5-080031
RP-39	RP-080113	0095		New MTSI test case 15.23 MO Explicit Communication Transfer	F	7.0.0	7.1.0	R5-080486
RP-39	RP-080113	0096		IMS test case 8.3 / Supported Header and expire rule during de-registration	F	7.0.0	7.1.0	R5-080518
RP-39	RP-080113	0097		Align via header for early IMS	F	7.0.0	7.1.0	R5-080542
RP-39	RP-080113	0098		New MTSI test case MO MTSI Text call	F	7.0.0	7.1.0	R5-080547
RP-39	RP-080113	0099		New MTSI test case Speech AMR, indicate all codec modes	F	7.0.0	7.1.0	R5-080558

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-39	RP-080113	0100		New MTSI test case Speech AMR-WB, indicate all codec modes	F	7.0.0	7.1.0	R5-080559
RP-39	RP-080113	0101		New MTSI test case MT Video, add speech remove speech	F	7.0.0	7.1.0	R5-080560
RP-39	RP-080113	0102		New MTSI test case MT Video, add speech remove video	F	7.0.0	7.1.0	R5-080561
RP-39	RP-080113	0103		Add generic secondary PDP context procedure	F	7.0.0	7.1.0	R5-080092
RP-39	RP-080113	0104		New MTSI test case for MO Consultative Explicit Communication Transfer	F	7.0.0	7.1.0	R5-080505
RP-39	RP-080113	0105		New MTSI test case for MT Consultative Explicit Communication Transfer	F	7.0.0	7.1.0	R5-080506
RP-40	RP-080375	0106		Updating references and ICSI statements related to MTSI	F	7.1.0	7.2.0	R5-081047
RP-40	RP-080375	0107		Fix to SDP handling in MTSI test case 16.3.	F	7.1.0	7.2.0	R5-081540
RP-40	RP-080375	0108		Branch value of Via header in MT messages	F	7.1.0	7.2.0	R5-081049
RP-40	RP-080375	0109		Introducing conditions for MO and MT versions of IMS common messages	F	7.1.0	7.2.0	R5-081050
RP-40	RP-080375	0110		New MTSI test case 15.6 Communication Deflection	F	7.1.0	7.2.0	R5-081539
RP-40	RP-080375	0111		New MTSI test case 15.17 Creating a conference	F	7.1.0	7.2.0	R5-081052
RP-40	RP-080375	0112		New MTSI test case 17.1 MO Speech add video remove video	F	7.1.0	7.2.0	R5-081541
RP-40	RP-080375	0113		New MTSI test case 15.5 Communication Forwarding unconditional	F	7.1.0	7.2.0	R5-081054
RP-40	RP-080375	0114		New MTSI test case 15.24 MT ECT - Blind Call Transfer	F	7.1.0	7.2.0	R5-081055
RP-40	RP-080375	0115		Update conformance requirement for TC 8.5	F	7.1.0	7.2.0	R5-081070
RP-40	RP-080375	0116		Update conformance requirement for TC 8.6	F	7.1.0	7.2.0	R5-081071
RP-40	RP-080375	0117		Update conformance requirement for TC 8.7	F	7.1.0	7.2.0	R5-081072
RP-40	RP-080375	0118		Update conformance requirement for TC 8.8	F	7.1.0	7.2.0	R5-081073
RP-40	RP-080375	0119		New MTSI test case MT MTSI Speech call	F	7.1.0	7.2.0	R5-081542
RP-40	RP-080375	0120		New MTSI test case MT MTSI Video call	F	7.1.0	7.2.0	R5-081543
RP-40	RP-080375	0121		New MTSI test case Speech AMR indicate selective codec modes	F	7.1.0	7.2.0	R5-081553
RP-40	RP-080375	0122		New MTSI test case Speech AMR-WB indicate selective codec modes	F	7.1.0	7.2.0	R5-081545
RP-40	RP-080375	0123		New MTSI test case MT Speech add video remove video	F	7.1.0	7.2.0	R5-081546
RP-40	RP-080375	0124		New MTSI test case MT Speech add video remove speech	F	7.1.0	7.2.0	R5-081547
RP-40	RP-080375	0125		Updating the content of the default INVITE message to Rel-7	F	7.1.0	7.2.0	R5-081537
RP-40	RP-080427	0126		Correction to 380 Alternative Service message	F	7.1.0	7.2.0	R5-081538
RP-41	RP-080563	0127		Add generic procedures for MTSI MT speech call, MT video call and MT text call	F	7.2.0	7.3.0	R5-083113
RP-41	RP-080563	0128		Update MTSI test case 12.13	F	7.2.0	7.3.0	R5-083114
RP-41	RP-080563	0129		Update MTSI test case 12.15	F	7.2.0	7.3.0	R5-083115
RP-41	RP-080563	0130		New MTSI test case 12.17 MT MTSI Text call	F	7.2.0	7.3.0	R5-083116
RP-41	RP-080563	0131		Update MTSI test case 16.1	F	7.2.0	7.3.0	R5-083126
RP-41	RP-080563	0132		Update MTSI test case 16.2	F	7.2.0	7.3.0	R5-083127
RP-41	RP-080563	0133		Update MTSI test case 16.3	F	7.2.0	7.3.0	R5-083128
RP-41	RP-080563	0134		Update MTSI test case 16.4	F	7.2.0	7.3.0	R5-083129
RP-41	RP-080563	0135		New MTSI test case 16.5 Video H.263 profile 0	F	7.2.0	7.3.0	R5-083130
RP-41	RP-080563	0136		New MTSI test case 16.6 Video H.263 profile 3	F	7.2.0	7.3.0	R5-083131
RP-41	RP-080563	0137		New MTSI test case 16.7 Video H.264	F	7.2.0	7.3.0	R5-083132
RP-41	RP-080563	0138		New MTSI test case 16.8 Video MPEG-4	F	7.2.0	7.3.0	R5-083133
RP-41	RP-080563	0139		Update MTSI test case 12.16	F	7.2.0	7.3.0	R5-083392
RP-41	RP-080557	0140		Removal of IMS test case 13.4	F	7.2.0	7.3.0	R5-083489
RP-41	RP-080563	0141		New MTSI test case 17.12 MT Video, add text	F	7.2.0	7.3.0	R5-083554
RP-41	RP-080563	0142		New MTSI test case 17.18 MT Text, add video	F	7.2.0	7.3.0	R5-083557
RP-41	RP-080563	0143		Addition of new MTSI test case for Originating Identification Presentation	F	7.2.0	7.3.0	R5-083558
RP-41	RP-080563	0144		Addition of new MTSI test case for Origination Identification Restriction	F	7.2.0	7.3.0	R5-083559
RP-41	RP-080563	0145		Update MTSI test case 17.2	F	7.2.0	7.3.0	R5-083627
RP-41	RP-080563	0146		Update MTSI test case 17.4	F	7.2.0	7.3.0	R5-083628
RP-41	RP-080563	0147		Update MTSI test case 17.8	F	7.2.0	7.3.0	R5-083629
RP-41	RP-080563	0148		Update MTSI test case 17.10	F	7.2.0	7.3.0	R5-083630
RP-41	RP-080563	0149		New MTSI test case 17.14 MT Text, add speech remove speech	F	7.2.0	7.3.0	R5-083631
RP-41	RP-080563	0150		New MTSI test case 17.16 MT Text, add speech remove text	F	7.2.0	7.3.0	R5-083632

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-41	RP-080563	0151		New MTSI test case 17.6 MT Speech, add text	F	7.2.0	7.3.0	R5-083119
RP-42	RP-080966	0152		Removing unnecessary exceptions from MTSI test case 12.4.	F	7.3.0	7.4.0	R5-085040
RP-42	RP-080966	0153		Updating generic requirements and XCAP test cases for XCAP authentication	F	7.3.0	7.4.0	R5-085041
RP-42	RP-080966	0154		New MTSI test case 15.14 Incoming Communication Barring for anonymous users	F	7.3.0	7.4.0	R5-085043
RP-42	RP-080966	0155		New MTSI test case 15.7 Communication Forwarding on non Reply: activation	F	7.3.0	7.4.0	R5-085044
RP-42	RP-080966	0156		New MTSI test case 15.21 Joining a conference after being invited to it	F	7.3.0	7.4.0	R5-085046
RP-42	RP-080966	0157		New MTSI test case 15.8 Communication Forwarding on non Reply: MO call initiation	F	7.3.0	7.4.0	R5-085047
RP-42	RP-080966	0158		Corrections to IMS CC test case 11.2 Network initiated re-authentication	F	7.3.0	7.4.0	R5-085050
RP-42	RP-080966	0159		Update 12.13 MT MTSI speech call	F	7.3.0	7.4.0	R5-085265
RP-42	RP-080966	0160		Update annex C.11 MTSI MT speech call	F	7.3.0	7.4.0	R5-085266
RP-42	RP-080966	0161		Add chapter headings for chapter 16 and 17	F	7.3.0	7.4.0	R5-085267
RP-42	RP-080966	0162		Correction to add the reference to the PICS statements in Annex A	F	7.3.0	7.4.0	R5-085341
RP-42	RP-080966	0163		Remove non MTSI related call setup test cases	F	7.3.0	7.4.0	R5-085350
RP-42	RP-080966	0164		Clarify GRUU applicability	F	7.3.0	7.4.0	R5-085351
RP-42	RP-080966	0165		Add generic procedures for MTSI MO speech call, call hold and conference call	F	7.3.0	7.4.0	R5-085405
RP-42	RP-080966	0166		New MTSI test case 16.10 MO MTSI Text session with MSRP	F	7.3.0	7.4.0	R5-085406
RP-42	RP-080966	0167		Update 16.1 Speech AMR, indicate all codec modes	F	7.3.0	7.4.0	R5-085426
RP-42	RP-080966	0168		Update 16.2 Speech AMR, indicate selective codec modes	F	7.3.0	7.4.0	R5-085427
RP-42	RP-080966	0169		Update 16.3 Speech AMR-WB, indicate all codec modes	F	7.3.0	7.4.0	R5-085428
RP-42	RP-080966	0170		Update 16.4 Speech AMR-WB, indicate selective codec mode	F	7.3.0	7.4.0	R5-085429
RP-42	RP-080966	0171		Update 17.2 MT Speech, add video remove video	F	7.3.0	7.4.0	R5-085432
RP-42	RP-080966	0172		Update of MTSI test cases for adding/removing media	F	7.3.0	7.4.0	R5-085443
RP-42	RP-080966	0173		New MTSI test case 15.18 Inviting user to conference by sending a REFER request to the user	F	7.3.0	7.4.0	R5-085445
RP-42	RP-080966	0174		Remove MTSI test cases for non mandatory use cases	F	7.3.0	7.4.0	R5-085446
RP-43	RP-090205	0175	-	Update of TS 34.229-1 from Rel-7 to Rel-8		7.4.0	8.0.0	R5-090763
RP-43	RP-090213	0202	-	IMS test case 8.9 / Supported Header and expire rule during de-registration		8.0.0	8.1.0	R5-090206
RP-43	RP-090213	0176	-	Addition of new MTSI test case for Terminating Identification Presentation		8.0.0	8.1.0	R5-090545
RP-43	RP-090213	0177	-	Addition of new MTSI test case for Terminating Identification Restriction		8.0.0	8.1.0	R5-090546
RP-43	RP-090213	0178	-	Updates to MTSI TCs 12.12 and 17.1 for MO speech and video		8.0.0	8.1.0	R5-090584
RP-43	RP-090213	0179	-	New MTSI test case 15.19 for inviting user to conference via conference focus		8.0.0	8.1.0	R5-090593
RP-43	RP-090213	0180	-	New MTSI test case 15.9 Communication Forwarding on Busy		8.0.0	8.1.0	R5-090594
RP-43	RP-090213	0181	-	New MTSI test case 15.10 Communication Forwarding not logged in		8.0.0	8.1.0	R5-090595
RP-43	RP-090213	0182	-	New MTSI test case 15.15 Subscription to the MWI event package		8.0.0	8.1.0	R5-090596
RP-43	RP-090213	0183	-	New MTSI test case 17.5 MO Speech, add text		8.0.0	8.1.0	R5-090597
RP-43	RP-090213	0184	-	Harmonizing the requirements within MTSI XCAP test cases		8.0.0	8.1.0	R5-090598
RP-43	RP-090213	0185	-	Add annex MTSI MT speech call, SS resources available		8.0.0	8.1.0	R5-090599
RP-43	RP-090213	0186	-	New MTSI test case 16.11		8.0.0	8.1.0	R5-090600
RP-43	RP-090213	0187	-	New MTSI test case 16.12		8.0.0	8.1.0	R5-090601
RP-43	RP-090213	0188	-	Remove video only based codec selection test cases		8.0.0	8.1.0	R5-090603
RP-43	RP-090213	0189	-	Update MTSI test case 17.2		8.0.0	8.1.0	R5-090613
RP-43	RP-090213	0190	-	Update MTSI test case 17.6		8.0.0	8.1.0	R5-090614
RP-43	RP-090213	0191	-	Update MTSI test case 17.18		8.0.0	8.1.0	R5-090615
RP-43	RP-090213	0192	-	Add annex MTSI MO text call		8.0.0	8.1.0	R5-090617
RP-43	RP-090213	0193	-	Update MTSI test case 12.16		8.0.0	8.1.0	R5-090618
RP-43	RP-090213	0194	-	New MTSI test case 17.17		8.0.0	8.1.0	R5-090619
RP-43	RP-090213	0195	-	Update annex C.11 MTSI MT speech call		8.0.0	8.1.0	R5-090620

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-43	RP-090214	0196	-	Update annex C.13 MTSI MT text call		8.0.0	8.1.0	R5-090621
RP-43	RP-090214	0197	-	Update MTSI test case 12.13		8.0.0	8.1.0	R5-090622
RP-43	RP-090214	0198	-	Update MTSI test case 12.17		8.0.0	8.1.0	R5-090623
RP-43	RP-090214	0199	-	New MTSI test case 16.13		8.0.0	8.1.0	R5-090660
RP-43	RP-090214	0200	-	Remove non MTSI related call setup test cases (2nd)		8.0.0	8.1.0	R5-090661
RP-43	RP-090214	0201	-	Remove MTSI test case 17.8		8.0.0	8.1.0	R5-090662
RP-44	RP-090433	0202	-	Update IMS test case 8.1, 8.2 and 8.6 with registration expire requirements		8.1.0	8.2.0	R5-092062
RP-44	RP-090433	0203	-	Update IMS test case 8.3 and 8.9 with registration expire requirements		8.1.0	8.2.0	R5-092063
RP-44	RP-090433	0204	-	Update IMS test case 8.5, 8.7 and 8.8 with registration expire requirements		8.1.0	8.2.0	R5-092064
RP-44	RP-090433	0205	-	Correction of registration expire requirements in annex A		8.1.0	8.2.0	R5-092065
RP-44	RP-090433	0206	-	Update of MTSI test case 15.15		8.1.0	8.2.0	R5-092217
RP-44	RP-090433	0207	-	Correction of MTSI icsi requirements		8.1.0	8.2.0	R5-092566
RP-45	RP-090794	0208	-	Update test cases 16.1, 16.2, 16.3 and 16.4 with multiple SDP check	F	8.2.0	8.3.0	R5-094352
RP-45	RP-090794	0209	-	Update annex C.13 and C.16 with multiple SDP check	F	8.2.0	8.3.0	R5-094353
RP-45	RP-090795	0210	-	Addition of P-Asserted-Identity header field to the 380 Alternative Service message	F	8.2.0	8.3.0	R5-094440
RP-46	RP-091118	0211		Update SDP speech offer for test case 12.13, annex C.11 and C.16	F	8.3.0	8.4.0	R5-095806
RP-46	RP-091118	0212	-	Update SDP speech offer for test cases 15.6	F	8.3.0	8.4.0	R5-095807
RP-46	RP-091118	0213	-	Update SDP speech offer for test cases 16.1, 16.2, 16.3 and 16.4	F	8.3.0	8.4.0	R5-095808
RP-46	RP-091118	0214	-	Update SDP speech offer for test cases 17.2 and 17.6	F	8.3.0	8.4.0	R5-095809
RP-46	RP-091118	0215	-	Correct gruu requirements in annex A	F	8.3.0	8.4.0	R5-095810
RP-46	RP-091116	0216	-	Update test case 14.2 with XML correction	F	8.3.0	8.4.0	R5-095812
RP-46	RP-091116	0217	-	Correct XML schema in 380 Alternative Service message	F	8.3.0	8.4.0	R5-095813
RP-46	RP-091118	0218	-	Update IMS test case 8.1, 8.5, 8.6 and 8.7 with registration expire corrections	F	8.3.0	8.4.0	R5-095816
RP-46	RP-091118	0219	-	Update IMS test case 8.1, 8.5, 8.6 and 8.7 with subscribe correction	F	8.3.0	8.4.0	R5-095817
RP-46	RP-091118	0220	-	Update test case 12.2	F	8.3.0	8.4.0	R5-096182
RP-46	RP-091118	0221	-	Update test cases 16.11, 16.12 and 16.13 with multiple SDP check	F	8.3.0	8.4.0	R5-096625
RP-46	RP-091118	0222	-	Update test cases 17.2, 17.6 and 17.18 with multiple SDP check	F	8.3.0	8.4.0	R5-096626
RP-47	RP-100155	0223	-	Add references for SMS over IP	F	8.4.0	8.5.0	R5-100505
RP-47	RP-100155	0224	-	Update message REGISTER for SMS	F	8.4.0	8.5.0	R5-100506
RP-47	RP-100155	0225	-	Update test case 8.1 for SMS	F	8.4.0	8.5.0	R5-100508
RP-47	RP-100155	0226	-	Add new test case 18.2 for SMS	F	8.4.0	8.5.0	R5-100509
RP-47	RP-100155	0227	-	Add default messages for SMS	F	8.4.0	8.5.0	R5-100785
RP-47	RP-100155	0228	1	Addition of new SMS over IMS test case 18.1	F	8.4.0	8.5.0	R5-101180
RP-47	-	-	-	Moved to v9.0.0 with no change	-	8.4.0	9.0.0	-
RP-48	RP-100511	0229	-	Update test cases 12.12 and 12.13 for AVP	F	9.0.0	9.1.0	R5-103485
RP-48	RP-100511	0230	-	Update generic procedure C.11 for AVP	F	9.0.0	9.1.0	R5-103490
RP-48	RP-100511	0231	-	Update test case 16.1 for AVP	F	9.0.0	9.1.0	R5-103492
RP-48	RP-100511	0232	-	Update test case 16.2 for AVP	F	9.0.0	9.1.0	R5-103493
RP-48	RP-100511	0233	-	Update test case 16.3 for AVP	F	9.0.0	9.1.0	R5-103494
RP-48	RP-100511	0234	-	Update test case 16.4 for AVP	F	9.0.0	9.1.0	R5-103495
RP-48	RP-100511	0235	-	Aligning MTSI MO call towards GSMA VoLTE profile	F	9.0.0	9.1.0	R5-103853
RP-48	RP-100511	0238	-	Aligning MTSI Call Hold test cases towards GSMA VoLTE profile	F	9.0.0	9.1.0	R5-103854
RP-48	RP-100511	0236	-	Adding media and NoReplyTimer elements to MTSI TC 15.7	F	9.0.0	9.1.0	R5-103855
RP-48	RP-100511	0237	-	GCF Priority 4 - Correction to annex A for TC 18.1 SMS over IMS	F	9.0.0	9.1.0	R5-103857
RP-49	RP-100985	0249	-	Add new test case for user initiated de-registration using GIBA	F	9.1.0	9.2.0	R5-104433
RP-49	RP-100985	0255	-	Add new test case 15.X Communication Waiting and answering the call	F	9.1.0	9.2.0	R5-104740
RP-49	RP-100985	0245	-	Add generic procedure for EPS bearer context activation	F	9.1.0	9.2.0	R5-104311
RP-49	RP-100986	0252	-	Add new test case 15.X Three way session creation	F	9.1.0	9.2.0	R5-104522
RP-49	RP-100986	0244	-	Add generic procedure for PDP context activation	F	9.1.0	9.2.0	R5-104310
RP-49	RP-100986	0248	-	Add new test case for initial registration using IMS	F	9.1.0	9.2.0	R5-104431

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
				AKA and GIBA against a network with GIBA support only				
RP-49	RP-100986	0247	-	Add new test case for initial registration using GIBA	F	9.1.0	9.2.0	R5-104430
RP-49	RP-100986	0242	-	Add new test case 15.x Communication Waiting and cancelling the call	F	9.1.0	9.2.0	R5-104292
RP-49	RP-100986	0253	-	Update generic procedures C.1, C.2 and C.2a	F	9.1.0	9.2.0	R5-104738
RP-49	RP-100986	0241	-	Add new test case 15.x Communication Forwarding not reachable	F	9.1.0	9.2.0	R5-104291
RP-49	RP-100986	0246	-	Remove clause 8 test cases for early IMS security	F	9.1.0	9.2.0	R5-104429
RP-49	RP-100986	0250	-	Update annex A for GIBA	F	9.1.0	9.2.0	R5-104434
RP-49	RP-100985	0251	-	Update test case 13.1	F	9.1.0	9.2.0	R5-104435
RP-49	RP-100986	0254	-	Add new test case for user initiated re-registration using GIBA	F	9.1.0	9.2.0	R5-104739
RP-49	RP-100986	0240	-	Correction to default Status Report for MO SMS	F	9.1.0	9.2.0	R5-104113
RP-49	RP-100985	0256	-	Changes to common messages for IMS emergency session setup	F	9.1.0	9.2.0	R5-105023
RP-49	RP-100838	0243	-	Update annex C.6	F	9.1.0	9.2.0	R5-104309
-	-	-	-	Editorial renumbering of test cases 15.27 - 15.30 in order to align with GCF list	-	9.1.0	9.2.0	-
RP-50	RP-101156	0260	-	Updates to conformance requirements related to IMS registration	F	9.2.0	9.3.0	R5-106152
RP-50	RP-101146	0258	-	Corrections to the conditions for using USIM or ISIM	F	9.2.0	9.3.0	R5-106150
RP-50	RP-101146	0259	-	Add new test case 15.14a Communication Barring while roaming	F	9.2.0	9.3.0	R5-106151
RP-50	RP-101146	0269	-	New Emergency test case 19.3.1 Non-UE detectable emergency call / IM CN sends a 1xx response / UE geographical location information available	F	9.2.0	9.3.0	R5-106590
RP-50	RP-101146	0268	-	Introducing TC 19.1.1 Basic IMS emergency call over EPS with emergency registration	F	9.2.0	9.3.0	R5-106586
RP-50	RP-101146	0262	-	Update of MTSI test cases 15.25 and 15.26	F	9.2.0	9.3.0	R5-106301
RP-50	RP-101146	0261	-	Update of MTSI test cases 15.1, 15.2, 15.3 and 15.4	F	9.2.0	9.3.0	R5-106300
RP-50	RP-101146	0264	-	Update to conformance requirement of PDP Context Activation test cases	F	9.2.0	9.3.0	R5-106470
RP-50	RP-101146	0263	-	Update conformance requirements for 8.10 and 8.11	F	9.2.0	9.3.0	R5-106452
RP-50	RP-101146	0267	-	Update test cases 9.1 and 9.2 to Rel-8	F	9.2.0	9.3.0	R5-106516
RP-50	RP-101146	0266	-	Remove test case 14.1 and 14.2	F	9.2.0	9.3.0	R5-106486
RP-50	RP-101156	0265	-	Update to conformance requirement of P-CSCF discovery test cases	F	9.2.0	9.3.0	R5-106472
RP-50	RP-101156	0257	-	Fixes to IMS common emergency messages	F	9.2.0	9.3.0	R5-106147
RP-50	RP-101146	0270	-	New IMS test case 12.2A MO Call - 504 Server Time-out	F	9.2.0	9.3.0	R5-106684
RP-51	RP-110165	0271	-	Updates to conformance requirements for XCAP and CDIV TCs	F	9.3.0	9.4.0	R5-110254
RP-51	RP-110165	0272	-	Updates to conformance requirements of IMS call related suppl. services	F	9.3.0	9.4.0	R5-110255
RP-51	RP-110165	0273	-	Updates to conformance requirements of IMS conference call TCs	F	9.3.0	9.4.0	R5-110256
RP-51	RP-110165	0274	-	Updates to conformance requirements of IMS MO calls	F	9.3.0	9.4.0	R5-110258
RP-51	RP-110165	0275	-	Updates to conformance requirements of IMS MO text session with MSRP	F	9.3.0	9.4.0	R5-110262
RP-51	RP-110174	0276	-	Corrections to the IMS emergency TC 19.1.1	F	9.3.0	9.4.0	R5-110265
RP-51	RP-110174	0277	-	Introducing TC 19.5.6 User-initiated emergency reregistration / UE has emergency related ongoing dialog	F	9.3.0	9.4.0	R5-110266
RP-51	RP-110174	0278	-	Introducing TC 19.1.2 Emergency call with emergency registration / Success / Location information not available	F	9.3.0	9.4.0	R5-110267
RP-51	RP-110174	0279	-	Introducing TC 19.1.4 Emergency call with emergency registration / UE is not [normal] registered / Success	F	9.3.0	9.4.0	R5-110268
RP-51	RP-110165	0280	-	Update test case 10.1	F	9.3.0	9.4.0	R5-110366
RP-51	RP-110165	0281	-	Update test case 12.2	F	9.3.0	9.4.0	R5-110367
RP-51	RP-110165	0282	-	Update test case 12.13	F	9.3.0	9.4.0	R5-110368
RP-51	RP-110165	0283	-	Update test case 12.16	F	9.3.0	9.4.0	R5-110369
RP-51	RP-110165	0284	-	Update test case 12.17	F	9.3.0	9.4.0	R5-110370
RP-51	RP-110165	0285	-	Update test case 16.1	F	9.3.0	9.4.0	R5-110374
RP-51	RP-110165	0286	-	Update test case 16.2	F	9.3.0	9.4.0	R5-110375
RP-51	RP-110165	0287	-	Update test case 16.3	F	9.3.0	9.4.0	R5-110376
RP-51	RP-110165	0288	-	Update test case 16.4	F	9.3.0	9.4.0	R5-110377
RP-51	RP-110165	0289	-	Add editor's note to test case 16.11	F	9.3.0	9.4.0	R5-110493

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-51	RP-110165	0290	-	Add editor's note to test case 16.12	F	9.3.0	9.4.0	R5-110494
RP-51	RP-110165	0291	-	Add editor's note to test case 16.13	F	9.3.0	9.4.0	R5-110495
RP-51	RP-110165	0292	-	Add editor's note to test case 17.2	F	9.3.0	9.4.0	R5-110496
RP-51	RP-110165	0293	-	Add editor's note to test case 17.6	F	9.3.0	9.4.0	R5-110497
RP-51	RP-110165	0294	-	Add editor's note to test case 17.17	F	9.3.0	9.4.0	R5-110498
RP-51	RP-110165	0295	-	Updating SMS related default messages and ISIM settings – 3 IMPU	F	9.3.0	9.4.0	R5-110673
RP-51	RP-110165	0296	-	Resubmission of new IMS test case 12.2A MO Call - 504 Server Time-out	F	9.3.0	9.4.0	R5-110689
RP-51	RP-110165	0297	-	Introducing new TC 7.9 P-CSCF discovery from ISIM	F	9.3.0	9.4.0	R5-110690
RP-51	RP-110165	0298	-	Correct service header fields in default MT INVITE	F	9.3.0	9.4.0	R5-110691
RP-51	RP-110165	0299	-	Support for multiple IMPU on ISIM	F	9.3.0	9.4.0	R5-110693
RP-51	RP-110165	0300	-	update test case 13.1	F	9.3.0	9.4.0	R5-110704
RP-51	RP-110165	0301	-	update test case 13.2	F	9.3.0	9.4.0	R5-110705
RP-51	RP-110165	0302	-	update test case 13.3	F	9.3.0	9.4.0	R5-110706
RP-51	RP-110174	0303	-	Introduction of new test case 19.1.3 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.3.0	9.4.0	R5-110804
RP-51	RP-110174	0304	-	Introduction of new test case 19.1.5 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.3.0	9.4.0	R5-110805
RP-51	RP-110174	0306	-	Introduction of new test case 19.4.3 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.3.0	9.4.0	R5-110807
RP-51	RP-110174	0307	-	Introduction of new test case 19.4.4 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.3.0	9.4.0	R5-110808
RP-51	RP-110174	0308	-	Update IMS emergency registration procedure	F	9.3.0	9.4.0	R5-110809
RP-51	RP-110174	0309	-	New emergency test case 19.3.2 Non-UE detectable emergency call / IM CN sends 380 Alternative Service / Non-emergency IMS registration	F	9.3.0	9.4.0	R5-110810
RP-52	RP-110660	0310	-	Removing references to MTSI from IMS emergency cal test cases	F	9.4.0	9.5.0	R5-112170
RP-52	RP-110660	0311	-	New TC 19.5.7 User-initiated emergency reregistration / The user initiates an emergency call	F	9.4.0	9.5.0	R5-112171
RP-52	RP-110660	0312	-	New TC 19.5.8 User-initiated emergency reregistration / Standalone transactions exist	F	9.4.0	9.5.0	R5-112172
RP-52	RP-110660	0313	-	New TC 19.5.9 In parallel emergency and non-emergency registrations	F	9.4.0	9.5.0	R5-112173
RP-52	RP-110660	0314	-	New TC 19.5.10 Deregistration upon emergency registration expiration	F	9.4.0	9.5.0	R5-112174
RP-52	RP-110651	0315	-	Removal of early IMS security in clause 6 test cases	F	9.4.0	9.5.0	R5-112401
RP-52	RP-110651	0316	-	Removal of early IMS security in clause 7 test cases	F	9.4.0	9.5.0	R5-112402
RP-52	RP-110660	0317	-	Corrections to test case 19.1.5	F	9.4.0	9.5.0	R5-112406
RP-52	RP-110651	0318	-	Add editors note to test case 17.18	F	9.4.0	9.5.0	R5-112441
RP-52	RP-110651	0319	-	Add generic procedure for E-UTRAN MO speech	F	9.4.0	9.5.0	R5-112488
RP-52	RP-110660	0320	-	Add generic procedure for E-UTRAN emergency speech	F	9.4.0	9.5.0	R5-112492
RP-52	RP-110660	0321	-	Add new test case 19.4.1	F	9.4.0	9.5.0	R5-112495
RP-52	RP-110651	0322	-	Replacing px_PublicUserIdentity with references to IMPUs on ISIM	F	9.4.0	9.5.0	R5-112644
RP-52	RP-110651	0323	-	New IMS TC 8.x Refresh for ISIM parameters	F	9.4.0	9.5.0	R5-112645
RP-52	RP-110660	0324	-	Introduction of new test case 19.5.1 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.4.0	9.5.0	R5-112649
RP-52	RP-110660	0325	-	Introduction of new test case 19.4.2 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.4.0	9.5.0	R5-112650
RP-52	RP-110660	0326	-	Introduction of new test case 19.4.5 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.4.0	9.5.0	R5-112651
RP-52	RP-110660	0310	-	Removing references to MTSI from IMS emergency cal test cases	F	9.4.0	9.5.0	R5-112170
RP-52	RP-110660	0311	-	New TC 19.5.7 User-initiated emergency reregistration / The user initiates an emergency call	F	9.4.0	9.5.0	R5-112171
RP-52	RP-110660	0312	-	New TC 19.5.8 User-initiated emergency reregistration / Standalone transactions exist	F	9.4.0	9.5.0	R5-112172
RP-52	RP-110660	0313	-	New TC 19.5.9 In parallel emergency and non-emergency registrations	F	9.4.0	9.5.0	R5-112173
RP-52	RP-110660	0314	-	New TC 19.5.10 Deregistration upon emergency registration expiration	F	9.4.0	9.5.0	R5-112174
RP-52	RP-110651	0315	-	Removal of early IMS security in clause 6 test cases	F	9.4.0	9.5.0	R5-112401
RP-52	RP-110651	0316	-	Removal of early IMS security in clause 7 test cases	F	9.4.0	9.5.0	R5-112402
RP-52	RP-110660	0317	-	Corrections to test case 19.1.5	F	9.4.0	9.5.0	R5-112406
RP-52	RP-110651	0318	-	Add editors note to test case 17.18	F	9.4.0	9.5.0	R5-112441
RP-52	RP-110651	0319	-	Add generic procedure for E-UTRAN MO speech	F	9.4.0	9.5.0	R5-112488
RP-52	RP-110660	0320	-	Add generic procedure for E-UTRAN emergency speech	F	9.4.0	9.5.0	R5-112492

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-52	RP-110660	0321	-	Add new test case 19.4.1	F	9.4.0	9.5.0	R5-112495
RP-52	RP-110651	0322	-	Replacing px_PublicUserIdentity with references to IMPUs on ISIM	F	9.4.0	9.5.0	R5-112644
RP-52	RP-110651	0323	-	New IMS TC 8.x Refresh for ISIM parameters	F	9.4.0	9.5.0	R5-112645
RP-52	RP-110660	0324	-	Introduction of new test case 19.5.1 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.4.0	9.5.0	R5-112649
RP-52	RP-110660	0325	-	Introduction of new test case 19.4.2 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.4.0	9.5.0	R5-112650
RP-52	RP-110660	0326	-	Introduction of new test case 19.4.5 for CT1 aspects of IMS emergency call over GPRS and EPS	F	9.4.0	9.5.0	R5-112651
RP-53	RP-111142	0327	-	Update generic procedure for MTSI MO speech	F	9.5.0	9.6.0	R5-113735
RP-53	RP-111145	0328	-	Update generic procedures for IMS emergency call	F	9.5.0	9.6.0	R5-113740
RP-53	RP-111145	0329	-	Update test case 19.4.1	F	9.5.0	9.6.0	R5-113741
RP-53	RP-111151	0330	-	Addition of new test case 12.18	F	9.5.0	9.6.0	R5-113742
RP-53	RP-111151	0331	-	Addition of new test case 12.20	F	9.5.0	9.6.0	R5-113745
RP-54	RP-111583	0332	-	IMS Route header correction	F	9.6.0	9.7.0	R5-115326
RP-54	RP-111583	0333	-	Update annex C.21	F	9.6.0	9.7.0	R5-115341
RP-54	RP-111583	0334	-	Update test case 8.14	F	9.6.0	9.7.0	R5-115342
RP-54	RP-111583	0335	-	Update test case 12.2	F	9.6.0	9.7.0	R5-115343
RP-54	RP-111583	0336	-	Update test case and numbering to 12.2a	F	9.6.0	9.7.0	R5-115344
RP-54	RP-111583	0337	-	Update test case 12.12	F	9.6.0	9.7.0	R5-115346
RP-54	RP-111583	0338	-	Update test case 12.13	F	9.6.0	9.7.0	R5-115349
RP-54	RP-111583	0339	-	Update test case 15.8	F	9.6.0	9.7.0	R5-115493
RP-54	RP-111583	0340	-	Update test case 15.12	F	9.6.0	9.7.0	R5-115500
RP-54	RP-111583	0341	-	Add editor's note to annex C.7	F	9.6.0	9.7.0	R5-115513
RP-54	RP-111583	0342	-	Update test case 15.23	F	9.6.0	9.7.0	R5-115524
RP-54	RP-111583	0343	-	Removal of an editor's note for ISIM REFRESH	F	9.6.0	9.7.0	R5-115665
RP-54	RP-111583	0344	-	Update test case 15.11	F	9.6.0	9.7.0	R5-115666
RP-54	RP-111583	0345	-	Update test case 15.21a	F	9.6.0	9.7.0	R5-115667
RP-54	RP-111583	0346	-	Update test case 15.25	F	9.6.0	9.7.0	R5-115668
RP-54	RP-111583	0347	-	Update test case 15.26	F	9.6.0	9.7.0	R5-115669
RP-54	RP-111591	0348	-	Updating E-UTRA procedures for IMS emergency test cases	F	9.6.0	9.7.0	R5-115671
RP-55	RP-120184	0351	-	Update default message INVITE for MO	F	9.7.0	9.8.0	R5-120387
RP-55	RP-120184	0352	-	Add generic procedure for SRVCC media removal	F	9.7.0	9.8.0	R5-120392
RP-55	RP-120184	0353	-	Update annex C.22	F	9.7.0	9.8.0	R5-120399
RP-55	RP-120192	0354	-	Update of IMS emergency call test cases 19.1.3 and 19.1.5	F	9.7.0	9.8.0	R5-120405
RP-55	RP-120192	0355	-	Update of IMS emergency call test case 19.5.1	F	9.7.0	9.8.0	R5-120407
RP-55	RP-120183	0356	-	GCF Priority X - Correction to the test procedure in the section of 7.3.4	F	9.7.0	9.8.0	R5-120678
RP-55	RP-120183	0357	-	GCF Priority X - Correction to the test procedure in the section of 7.4.4, 7.5.4 and 7.6.4	F	9.7.0	9.8.0	R5-120679
RP-55	RP-120183	0358	-	GCF Priority X - Correction to the test procedures of the section of 12.2 and 12.2a	F	9.7.0	9.8.0	R5-120680
RP-55	RP-120183	0359	-	GCF Priority X - Correction to the message content in the section of 13.2.4	F	9.7.0	9.8.0	R5-120681
RP-55	RP-120183	0360	-	GCF Priority X - Correction to the testing sequence numberings in the sections of 15.21a and 15.23	F	9.7.0	9.8.0	R5-120682
RP-55	RP-120183	0361	-	GCF Priority X - Correction to the testing sequence numberings in the sections of 15.27	F	9.7.0	9.8.0	R5-120683
RP-55	RP-120183	0362	-	GCF Priority X - Correction to the testing content of 17.17.4	F	9.7.0	9.8.0	R5-120684
RP-55	RP-120171	0363	-	GCF Priority X - Correction to the reference index	F	9.7.0	9.8.0	R5-120685
RP-55	RP-120184	0364	-	Update default message 183 Session Progress	F	9.7.0	9.8.0	R5-120686
RP-55	RP-120192	0365	-	Update of IMS emergency call test cases 19.4.x	F	9.7.0	9.8.0	R5-120691
RP-55	RP-120195	0366	-	Addition of new test case 12.19	F	9.7.0	9.8.0	R5-120722
RP-56	RP-120649	0367	-	Update test case 12.12	F	9.8.0	9.9.0	R5-121423
RP-56	RP-120649	0368	-	Update test case 12.13	F	9.8.0	9.9.0	R5-121424
RP-56	RP-120655	0369	-	Removing TC 19.1.4 from 34.229-1	F	9.8.0	9.9.0	R5-121430

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-56	RP-120649	0370	-	Correction of XCAP MIME definition	F	9.8.0	9.9.0	R5-121629
RP-56	RP-120649	0371	-	Addition of new test case - MO MTSI Video Call	F	9.8.0	9.9.0	R5-121631
RP-56	RP-120649	0372	-	Addition of new test case - MT MTSI Video Call	F	9.8.0	9.9.0	R5-121633
RP-56	RP-120649	0373	-	Updates to 17.1 - MO Speech, add video remove video	F	9.8.0	9.9.0	R5-121635
RP-56	RP-120649	0374	-	Updates to 17.2 - MT Speech, add video remove video	F	9.8.0	9.9.0	R5-121636
RP-56	RP-120649	0375	-	Add generic procedure MT Video call for EPS	F	9.8.0	9.9.0	R5-121657
RP-56	RP-120648	0376	-	MO Message content correction for SMS-over-IMS	F	9.8.0	9.9.0	R5-121675
RP-56	RP-120649	0377	-	Add generic procedure MO video call for EPS	F	9.8.0	9.9.0	R5-121803
RP-56	RP-120655	0378	-	Correction to IMS emergency test case 19.3.2	F	9.8.0	9.9.0	R5-121804
RP-56	RP-120655	0379	-	New test case 19.3.3 Non-UE detectable emergency call / IM CN sends 380 Alternative Service / Emergency IMS registration	F	9.8.0	9.9.0	R5-121805
RP-56	RP-120655	0380	-	New test case 19.3.4 Non-UE detectable emergency call / IM CN sends 380 Alternative Service / Emergency IMS registration exists	F	9.8.0	9.9.0	R5-121806
RP-56	RP-120657	0381	-	Update the default messages and generic test procedures	F	9.8.0	9.9.0	R5-121851
RP-56	RP-120657	0382	-	Update to test case 12.19	F	9.8.0	9.9.0	R5-121852
RP-57	RP-121102	0383	-	IMS MTSI message content correction	F	9.9.0	9.10.0	R5-123077
RP-57	RP-121103	0384	-	Update to test case 12.19	F	9.9.0	9.10.0	R5-123200
RP-57	RP-121103	0385	-	Update generic procedure C.21	F	9.9.0	9.10.0	R5-123505
RP-57	RP-121103	0386	-	Update generic procedure C.25	F	9.9.0	9.10.0	R5-123525
RP-57	RP-121103	0387	-	Update generic procedure C.26	F	9.9.0	9.10.0	R5-123681
RP-57	RP-121103	0388	-	Update the default messages for IMS video	F	9.9.0	9.10.0	R5-123682
RP-57	RP-121103	0389	-	Updates to 17.1 - MO Speech, add video remove video	F	9.9.0	9.10.0	R5-123683
RP-57	RP-121103	0390	-	Updates to 17.2 - MT Speech, add video remove video	F	9.9.0	9.10.0	R5-123684
RP-58	RP-121663	0391	-	Correction of default message contents in Annex A	F	9.10.0	9.11.0	R5-125288
RP-58	RP-121663	0392	-	Correction of 11.2	F	9.10.0	9.11.0	R5-125289
RP-58	RP-121664	0393	-	Correction to references	F	9.10.0	9.11.0	R5-125575
RP-58	RP-121664	0394	-	Updates to 12-21 - MO MTSI Video call	F	9.10.0	9.11.0	R5-125578
RP-58	RP-121664	0395	-	Updates to 12-22 - MT MTSI Video call	F	9.10.0	9.11.0	R5-125579
RP-58	RP-121664	0396	-	Updates to 17.1 - MO Speech, add video remove video	F	9.10.0	9.11.0	R5-125580
RP-58	RP-121664	0397	-	Updates to 17.2 - MT Speech, add video remove video	F	9.10.0	9.11.0	R5-125581
RP-58	RP-121664	0398	-	Update test case 19.5.6	F	9.10.0	9.11.0	R5-125588
RP-58	RP-121664	0399	-	Update test case 19.5.1	F	9.10.0	9.11.0	R5-125589
RP-58	RP-121664	0400	-	Update test case 19.5.7	F	9.10.0	9.11.0	R5-125590
RP-58	RP-121664	0401	-	Update test case 19.5.8	F	9.10.0	9.11.0	R5-125591
RP-58	RP-121664	0402	-	Update test case 19.5.10	F	9.10.0	9.11.0	R5-125592
RP-58	RP-121664	0403	-	Update test case 19.3.1	F	9.10.0	9.11.0	R5-125595
RP-58	RP-121664	0404	-	Update test case 19.1.5	F	9.10.0	9.11.0	R5-125616

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-58	RP-121664	0405	-	Removal of location accuracy requirement from Emergency Services test cases	F	9.10.0	9.11.0	R5-125771
RP-58	RP-121664	0406	-	Update generic procedure C.11	F	9.10.0	9.11.0	R5-125772
RP-58	RP-121663	0407	-	IMS MTSI TC 15.28 correction	F	9.10.0	9.11.0	R5-125773
RP-58	RP-121663	0408	-	IMS MTSI TC 15.8 correction	F	9.10.0	9.11.0	R5-125774
RP-58	RP-121664	0411	-	Location stimulus clarification for Emergency Services test cases	F	9.10.0	9.11.0	R5-126025
RP-58	RP-121663	0412	-	IMS extend IMS_CC test case 8.1 for LTE	F	9.10.0	9.11.0	R5-126033
RP-58	RP-121663	0413	-	IMS Default content of ACK	F	9.10.0	9.11.0	R5-126034
RP-58	RP-121685	0409	-	Update the default messages for aSRVCC	F	9.11.0	10.0.0	R5-126003
RP-58	RP-121685	0410	-	Addition of new generic test procedures for aSRVCC	F	9.11.0	10.0.0	R5-126004
RP-59	RP-130145	0414	-	Correction to reference for IMS video related capability defined in TS 34.229-2	F	10.0.0	10.1.0	R5-130083
RP-59	RP-130143	0416	-	Update test case 12.21	F	10.0.0	10.1.0	R5-130491
RP-59	RP-130143	0417	-	Update test case 12.22	F	10.0.0	10.1.0	R5-130495
RP-59	RP-130143	0418	-	Update annex C.11	F	10.0.0	10.1.0	R5-130497
RP-59	RP-130143	0419	-	Correction to default settings of EF IMPU at ISIM ADF	F	10.0.0	10.1.0	R5-130519
RP-59	RP-130143	0420	-	Corrections to IMS_CC test case 8.4	F	10.0.0	10.1.0	R5-130548
RP-59	RP-130145	0421	-	Updates to conformance requirements in 19.1.1.2, 19.1.3.2, 19.1.5.2	F	10.0.0	10.1.0	R5-130566
RP-59	RP-130145	0422	-	Corrections to 19.5.6, 19.5.7, 19.5.8, A.1.1	F	10.0.0	10.1.0	R5-130567
RP-59	RP-130145	0423	-	Update A.7.2 MESSAGE for delivery report	F	10.0.0	10.1.0	R5-130572
RP-59	RP-130143	0424	-	Correction of 15 series of SS tests	F	10.0.0	10.1.0	R5-130678
RP-59	RP-130143	0425	-	Update test case 17.1	F	10.0.0	10.1.0	R5-130679
RP-59	RP-130143	0426	-	Update test case 17.2	F	10.0.0	10.1.0	R5-130680
RP-59	RP-130145	0427	-	Corrections to A.2.7	F	10.0.0	10.1.0	R5-130682
RP-59	RP-130145	0428	-	Corrections to A.3.1	F	10.0.0	10.1.0	R5-130683
RP-59	RP-130145	0429	-	Update default message MESSAGE for MO SMS	F	10.0.0	10.1.0	R5-130684
RP-59	RP-130145	0430	-	Update A.7.6 Delivery report for MO SMS	F	10.0.0	10.1.0	R5-130685
RP-59	RP-130143	0431	-	Update Annex A, C	F	10.0.0	10.1.0	R5-130750
RP-59	RP-130143	0432	-	Correction to SDP parameter in Generic Procedures in Annex C	F	10.0.0	10.1.0	R5-130751
RP-60	R5-131132	0433	-	Correction of TC 15.1	F	10.1.0	10.2.0	R5-131132
RP-60	R5-131134	0434	-	Update Annex A.1	F	10.1.0	10.2.0	R5-131134
RP-60	R5-131135	0435	-	Add new generic procedures in Annex C.29 for Supplementary Services test	F	10.1.0	10.2.0	R5-131135
RP-60	R5-131138	0436	-	TC 19.1.3a & 19.3.2a - split 1xRTT from UTRA, GERAN	F	10.1.0	10.2.0	R5-131138
RP-60	R5-131167	0437	-	Update to test function Update UE Location Information	F	10.1.0	10.2.0	R5-131167
RP-60	R5-131170	0438	-	Add missing references	F	10.1.0	10.2.0	R5-131170
RP-60	R5-131269	0439	-	Misc changes for TC 18.1	F	10.1.0	10.2.0	R5-131269
RP-60	R5-131292	0440	-	TCP as normative DL transport protocol in IMS Registration test	F	10.1.0	10.2.0	R5-131292
RP-60	R5-131875	0441	-	Update test case 8.4	F	10.1.0	10.2.0	R5-131875

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-60	R5-131887	0442	-	Expiry value in 200 OK	F	10.1.0	10.2.0	R5-131887
RP-60	R5-131897	0443	-	to-tag in ACK	F	10.1.0	10.2.0	R5-131897
RP-60	R5-132037	0444	-	Addition of new generic procedure in C.30 for Mobile Initiated IMS Deregistration	F	10.1.0	10.2.0	R5-132037
RP-60	R5-132038	0445	-	Correction of TC 8.2	F	10.1.0	10.2.0	R5-132038
RP-60	R5-132063	0446	-	To-tag in 202 Accepted	F	10.1.0	10.2.0	R5-132063
RP-60	R5-132064	0447	-	Record-Route header in A.2.3 on 183 Session Progress for INVITE	F	10.1.0	10.2.0	R5-132064
RP-60	R5-132065	0448	-	Fix step numbering in 9.2.4	F	10.1.0	10.2.0	R5-132065
RP-60	R5-132068	0449	-	Correction of TC 15.8	F	10.1.0	10.2.0	R5-132068
RP-61	RP-131100	0450	-	Correction to reference to RFC 6442	F	10.2.0	10.3.0	R5-133151
RP-61	RP-131100	0451	-	Correction to PRACK default message contents	F	10.2.0	10.3.0	R5-133188
RP-61	RP-131100	0452	-	Correction of TC 15 series	F	10.2.0	10.3.0	R5-133197
RP-61	RP-131100	0453	-	Correction of Annex C.29	F	10.2.0	10.3.0	R5-133198
RP-61	RP-131100	0454	-	Add MMI command releasing call in TC 12.12	F	10.2.0	10.3.0	R5-133301
RP-61	RP-131100	0455	-	Referring to generic procedure C.30 in TC 8.3	F	10.2.0	10.3.0	R5-133302
RP-61	RP-131100	0456	-	Correction of A.2.7	F	10.2.0	10.3.0	R5-133303
RP-61	RP-131100	0457	-	Clarification of A.2.9	F	10.2.0	10.3.0	R5-133304
RP-61	RP-131100	0458	-	Correction of C.30	F	10.2.0	10.3.0	R5-133305
RP-61	RP-131100	0459	-	Correction of the magic cookie value in Via branch as per the RFC 3261 definition	F	10.2.0	10.3.0	R5-133355
RP-61	RP-131100	0460	-	Restricting usage of rport to UDP as transport protocol	F	10.2.0	10.3.0	R5-133358
RP-61	RP-131100	0461	-	Correction to IMS Deregistration procedure in case of using TCP	F	10.2.0	10.3.0	R5-133578
RP-61	RP-131100	0462	-	Corrections to allow both ISIM or USIM to be used in IMS CC test cases	F	10.2.0	10.3.0	R5-133628
RP-61	RP-131100	0463	-	Correction of Option tags to indicate support of '100rel' and/or 'precondition'	F	10.2.0	10.3.0	R5-133629
RP-61	RP-131100	0464	-	Updating conformance requirements for test case 18.1	F	10.2.0	10.3.0	R5-133630
RP-61	RP-131100	0465	-	Clarification on SDP messages and SIP signalling of C.21	F	10.2.0	10.3.0	R5-133684
RP-61	RP-131100	0466	-	Clarification on SDP messages of C.13	F	10.2.0	10.3.0	R5-133703
RP-61	RP-131100	0467	-	Corrections to SMS over IMS test cases	F	10.2.0	10.3.0	R5-133705
RP-62	RP-131861	0468	-	Correction to MESSAGE default contents for SMS over IMS	F	10.3.0	10.4.0	R5-134094
RP-62	RP-131861	0469	-	Correction to default contents of 100 Trying response	F	10.3.0	10.4.0	R5-134095
RP-62	RP-131861	0470	-	Editorial corrections and clarifications to test case 15.11	F	10.3.0	10.4.0	R5-134114
RP-62	RP-131861	0471	-	Editorial corrections and clarifications to test case 15.8	F	10.3.0	10.4.0	R5-134115
RP-62	RP-131861	0472	-	Corrections for A.2.8 (BYE)	F	10.3.0	10.4.0	R5-134116
RP-62	RP-131861	0473	-	Correction of expected sequence of C.26	F	10.3.0	10.4.0	R5-134118
RP-62	RP-131861	0474	-	Clarification on SDP messages of C.11	F	10.3.0	10.4.0	R5-134119
RP-62	RP-131875	0475	-	Editorial corrections for SMS default message content	F	10.3.0	10.4.0	R5-134120
RP-62	RP-131875	0476	-	Update C.11 for IR.92 version 7	F	10.3.0	10.4.0	R5-134270
RP-62	RP-131875	0477	-	Clarify check of encrypt-algorithm in annex A.	F	10.3.0	10.4.0	R5-134287

Meeting -1st-Level	Doc-1st-Level	CR	Rev	Subject	Cat	Version-Current	Version-New	Doc-2nd-Level
RP-62	RP-131863	0478	-	Remove not needed test cases	F	10.3.0	10.4.0	R5-134297
RP-62	RP-131863	0479	-	Correction of Emergency Service over IMS test case 19.1.3	F	10.3.0	10.4.0	R5-134385
RP-62	RP-131863	0480	-	Correction of Emergency Service over IMS test case 19.5.7	F	10.3.0	10.4.0	R5-134386
RP-62	RP-131861	0481	-	Correction of Emergency Service over IMS test case 19.5.8	F	10.3.0	10.4.0	R5-134387
RP-62	RP-131875	0482	-	Corrections and clarifications to C.29.1	F	10.3.0	10.4.0	R5-134455
RP-62	RP-131875	0483	-	Update annex C for SDP	F	10.3.0	10.4.0	R5-134617
RP-62	RP-131875	0484	-	Update annex A for SDP	F	10.3.0	10.4.0	R5-134627
RP-62	RP-131875	0485	-	Clarify SDP in annex C.21	F	10.3.0	10.4.0	R5-134630
RP-62	RP-131875	0486	-	Update test case 17.2	F	10.3.0	10.4.0	R5-134646
RP-62	RP-131875	0487	-	Update annex C.11 according AP#60.08	F	10.3.0	10.4.0	R5-134648
RP-62	RP-131861	0488	-	Correction to default messages	F	10.3.0	10.4.0	R5-134659
RP-62	RP-131861	0489	-	Enhancement of C.8 to support Call Resume	F	10.3.0	10.4.0	R5-134793
RP-62	RP-131861	0490	-	Editorial correction for C.22	F	10.3.0	10.4.0	R5-134795
RP-62	RP-131861	0491	-	Correction of expected sequence of 16.1 and 16.3	F	10.3.0	10.4.0	R5-134796
RP-62	RP-131863	0492	-	Correction of expected sequence of C.13	F	10.3.0	10.4.0	R5-134797
RP-62	RP-131863	0493	-	Alignment of IMS message definitions with RFC6442	F	10.3.0	10.4.0	R5-134798
RP-62	RP-131861	0494	-	Correction to Annex A.2.1 and A.2.3 IMS message for Emergency Call NoRegistration	F	10.3.0	10.4.0	R5-134955
RP-62	RP-131861	0495	-	Correction to contents of ACK in test case 12.2	F	10.3.0	10.4.0	R5-134958
RP-62	RP-131891	0496	-	Correction of rtpmap attributes for media in SDP answer	F	10.3.0	10.4.0	R5-134961
RP-62	RP-131861	0498	-	Record-Route header	F	10.3.0	10.4.0	R5-135004
RP-62	RP-131875	0499	-	Update C.21 for IR.92 version 7	F	10.3.0	10.4.0	R5-135020

History

Document history		
V10.0.0	January 2013	Publication
V10.1.0	April 2013	Publication
V10.2.0	July 2013	Publication
V10.3.0	October 2013	Publication
V10.4.0	January 2014	Publication