ETSI TS 134 229-5 V15.1.0 (2020-11)

5G;
Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP);
User Equipment (UE) conformance specification;
Part 5: Protocol conformance specification using 5G System (5GS)
(3GPP TS 34.229-5 version 15.1.0 Release 15)

Reference
RTS/TSGR-0534229-5vf10

Keywords
5G

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

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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 (https://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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Legal Notice

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. These shall be interpreted as being references to the corresponding ETSI deliverables.

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

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.

In the present document, certain modal verbs have the following meanings:

shall indicates a mandatory requirement to do something

shall not indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

should indicates a recommendation to do something

should not indicates a recommendation not to do something

may indicates permission to do something

need not indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

can indicates that something is possible

cannot indicates that something is impossible

The constructions "can" and "cannot" shall not to be used as substitutes for "may" and "need not".

will indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

will not indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

might indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

might not indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

is (or any other verb in the indicative mood) indicates a statement of fact

is not (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

Introduction

The present document is the fifth part of a multi-part conformance specification valid for 3GPP Release 15 and later releases:

3GPP TS 34.229-1 [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 1: Protocol conformance specification".

3GPP TS 34.229-2 [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 2: Implementation Conformance Statement (ICS) proforma specification".

3GPP TS 34.229-3 [4]: "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)".

3GPP TS 34.229-4 [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 4: Enabler for IP multimedia applications testing".

3GPP TS 34.229-5 (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 5: Protocol conformance specification using 5G System (5GS)".

NOTE 1: The ATS is written in a standard testing language, TTCN-3, as defined in ETSI ES 201 873, Parts 1 to 3 [8], [9] and [10].

NOTE 2: Further information on testing can be found in ETSI ETS 300 406 [11] and ISO/IEC 9646-1 [12].

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 [4]).

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) when using the 5G System (5GS).

This is the fifth 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
- the test procedure.

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

- Implementation Conformance Statement (ICS) pro-forma and the applicability of each test case [3].

The present document is valid for UE implemented according to 3GPP Releases starting from Release 15 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*.

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

[2] 3GPP TS 34.229-1: "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".

[3] 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".

[4] 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)".

[5] 3GPP TS 34.229-4: "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); User Equipment (UE) conformance specification; Part 4: Enabler for IP multimedia applications testing".

[6] IETF RFC 3261: "SIP: Session Initiation Protocol".

[7] 3GPP TS 24.229: "IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[8] 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".

[9] 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)".

[10] 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)".

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

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

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

[14] 3GPP TS 24.341: "Support of SMS over IP networks; Stage 3".

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

[16] 3GPP TS 33.203: "3G security;Access security for IP-based services".

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

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

[19] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[20] 3GPP TS 24.501: "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3".

[21] 3GPP TS 38.508-1: "5GS; User Equipment (UE) conformance specification; Part 1: Common test environment".

[22] 3GPP TS 27.007: "AT command set for User Equipment (UE)".

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

[24] 3GPP TS 23.040: "Technical realization of the Short Message Service (SMS)".

[25] 3GPP TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[26] 3GPP TS 24.237: "IP Multimedia (IM) Core Network (CN) subsystem IP Multimedia Subsystem (IMS) Service Continuity".

[27] 3GPP TS 23.003: "Numbering, addressing and identification".

3 Definitions of terms, symbols and abbreviations

3.1 Terms

Void

3.2 Symbols

Void

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

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 [13] 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 clause of the test body refers to clauses in the referred specification, not clauses in the present document.

5 Reference Conditions

5.1 General

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.

5.2 Generic setup procedures

A set of basic generic procedures for different IMS usage scenarios are described in Annex A of this specification. These procedures are used in numerous test cases throughout the present document. Default Messages are used from and maintained in Annex A of TS 34.229-1 [2].

5.3 Transport protocols applied

For simplicity, UDP (*User Datagram Protocol*) is applied to IMS testing as default DL transport protocol, except for the test cases in clause 6 where TCP (*Transmission Control Protocol*) is applied as DL transport protocol.

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

6 Registration

6.1 Initial Registration / 5GS

6.1.1 Test Purpose (TP)

(1)

```
with { UE has an ISIM or USIM inserted, is registered for 5GS, and has acquired P-CSCF address(es) }
ensure that {
  when { UE is made to register for IMS }
   then { UE sends a correctly composed initial REGISTER request to the P-CSCF }
            }
```

(2)

```
with { UE having sent unprotected REGISTER request }
ensure that {
  when { UE receiving a valid 401 (Unauthorized) response for the initial REGISTER request sent }
   then { UE correctly authenticates itself by sending another REGISTER request with a correctly
composed Authorization header using the AKAv1-MD5 algorithm }
            }
```

(3)

```
with { UE having sent unprotected and then protected REGISTER request }
ensure that {
  when { UE receiving a valid 200 OK response from S-CSCF for the REGISTER sent for authentication }
   then { UE subscribes to the reg event package for the public user identity registered, using the
stored service route for routing the SUBSCRIBE request }
            }
```

(4)

```
with { UE having subscribed to reg event }
ensure that {
  when { UE receives NOTIFY request for reg event }
   then { UE responds with a valid 200 OK response }
            }
```

6.1.2 Conformance Requirements

[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 TS 23.003 [3]. 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 TS 33.203 [19]. See also clause 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 [19].

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, UE-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 field.

If the UE is unable to derive the parameters in this clause 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.

...

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 [26].

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 to use 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:

...

2) the public user identity to be registered;

b) a To header field set to the SIP URI that contains:

...

2) 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:

1) supports GRUU (see table A.4, item A.4/53);

...

3) has an IMEI available; or

...

the UE shall include a "+sip.instance" header field parameter containing the instance ID. ...

NOTE 2: The requirement placed on the UE to include an instance ID based on the IMEI or the MEID when the UE does not support GRUU and does not support multiple registrations does not imply any additional requirements on the network.

...

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 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 [62].

The UE shall include the media feature tags as defined in RFC 3840 [62] for all supported streaming media types.

...

If the UE has no specific reason not to include a user part in the URI of the contact address (e.g. some UE performing the functions of an external attached network), the UE should include a user part in the URI of the contact address such that the user part is globally unique and does not reveal any private information;

NOTE 3: A time-based UUID (Universal Unique Identifier) generated as per subclause 4.2 of RFC 4122 [154] is globally unique and does not reveal any private information.

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 UDP is 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 RFC 6223 [143];

NOTE 4: 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 5: 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);

...

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 either to the respective contact address of the UE or to the registration flow and the associated contact address (if the multiple registration mechanism is used);

...

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;

...

d) store the list of service route values contained in the Service-Route header field and bind the list either to the contact address or to the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session over which the REGISTER request was sent;

NOTE 10: When multiple registration mechanism is not used, there will be only one list of service route values bound to a contact address. However, when multiple registration mechanism is used, there will be different list of service route values bound to each registration flow and the associated contact address.

NOTE 11: The UE will use the stored list of service route values to build a proper preloaded Route header field for new dialogs and standalone transactions (other than REGISTER method) when using either the respective contact address or the registration flow and the associated contact address (if the multiple registration mechanism is used), and the associated set of security associations or TLS session.

e) if the UE indicated support for GRUU in the Supported header field of the REGISTER request then:

- if the UE did not use the procedures specified in RFC 6140 [191] for registration, 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, 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; and

...

NOTE 12: When allocating public GRUUs to registering UAs the functionality within the UE that performs the role of registrar will add an "sg" SIP URI parameter that uniquely identifies that UA to the public GRUU it received in the "pub-gruu" header field parameter. The procedures for generating a temporary GRUU using the "temp-gruu-cookie" header field parameter are specified in subclause 7.1.2.2 of RFC 6140 [191].

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 [92], and the S-CSCF has followed the registration procedure as described in RFC 5627 [93] or RFC 3261 [26], 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 [92], the UE shall refrain from registering any additional IMS flows for the same private identity as described in RFC 5626 [92]; or

NOTE 13: 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 [92];

g) if available, store the announcement of media plane security mechanisms the P-CSCF (IMS-ALG) supports labelled with the "mediasec" header field parameter specified in subclause 7.2A.7 and received in the Security-Server header field, if any. Once the UE chooses a media security mechanism from the list received in the Security-Server header field from the server, it may initiate that mechanism on a media level when it initiates new media in an existing session;

NOTE 14: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

[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 [19].

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 [19]. The syntax of the parameters needed for the security association setup is specified in annex H of 3GPP TS 33.203 [19]. The UE shall support the "ipsec-3gpp" security mechanism, as specified in RFC 3329 [48]. The UE shall support the IPsec layer algorithms for integrity and confidentiality protection as defined in 3GPP TS 33.203 [19], and shall announce support for them according to the procedures defined in RFC 3329 [48].

[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 [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;

...

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.

NOTE 2: The Security-Client header field contains signalling plane security mechanism and if the UE supports media plane security, then media plane security mechanisms are contained, too.

[TS 24.229, clause 5.1.1.5.1]:

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 3: 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 [43] and RFC 6665 [28].

...

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.

NOTE 2: The subscription information stored in the HSS ensures that the default public user identity is a SIP URI.

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 the SIP URI that is the default public user identity used for subscription;

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

c) a To header field set to the SIP URI that is the default 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 5.1.2.1]:

Upon receipt of a NOTIFY request for the dialog associated with the subscription to the reg event package the UE shall perform the following actions:

- store the information for the established dialog;

- store the expiration time as indicated in the "expires" header field parameter of the Subscription-State header field, if present, of the NOTIFY request. Otherwise the expiration time is retrieved from the Expires header field of the 2xx response to SUBSCRIBE request;

- if a <registration> element with 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 <registration> element with 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 [94]), the UE shall store the value of those elements in association with the public user identity;

[TS 24.229, clause 5.1.2A.1.1]:

When the UE sends any request, the UE shall use either a given contact address that has been previously registered or a registration flow and the associated contact address (if the multiple registration mechanism is used) and 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;

...

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;

...

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 [93]; 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 [93];

- otherwise, a SIP URI containing the contact address of the UE that has been previously registered without any contact parameters dedicated to registration procedure;

NOTE 7: The above items are mutually exclusive.

...

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 CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method (see subclause 7.2A.4). Insertion of the P-Access-Network-Info header field into the ACK request is optional.

NOTE 13: 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).

NOTE 14: The value of the P-Access-Network-Info header field could be stale if the point of attachment of the UE with the network changes before the message is received by the network.

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 acquired at the time of the P-CSCF discovery procedures which was used in registration of the contact address (or registration flow); and

NOTE 15: If the UE is provisioned with or receives a FQDN at the time of the P-CSCF discovery procedures, the FQDN is resolved to an IP address at the time of the P-CSCF discovery procedures.

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;

...

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.

NOTE 16: When the UE registers multiple contact addresses, there will be a list of Service-Route headers for each contact address. When sending a request using a given contact address and the associated security associations or TLS session, the UE will use the corresponding list of Service-Route headers to construct a list of Route headers.

[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 [16].

6.1.3 Test description

6.1.3.1 Pre-test conditions

System Simulator:

- 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 IMS AKA authentication for the IMPI, according to 3GPP TS 33.203 [16] clause 6.1.
- 1 NR Cell

UE:

- The UE contains either ISIM and USIM applications or only USIM application on UICC.
- The UE is configured to register for IMS after switch on.
- The UE is switched off.

Preamble:

- None

6.1.3.2 Test procedure sequence

Table 6.1.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	The UE is switched on.				
2	Check: does the UE send an initial registration request?	-->	REGISTER	1	P
3	SS sends 401 Unauthorized.	<--	401 Unauthorized		
4	Check: does the UE send a subsequent registration request?	-->	REGISTER	2	P
5	SS sends 200 OK for REGISTER.	<--	200 OK		
	EXCEPTION: In parallel to the events described in steps 6 to 9, the steps specified in Table 6.1.3.2-2 may take place.				
6	Check: does the UE subscribe to reg-event?	-->	SUBSCRIBE	3	P
7	SS sends 200 OK for SUBSCRIBE.	<--	200 OK		
8	SS sends NOTIFY for reg-event package.	<--	NOTIFY		
9	Check: does the UE acknowledge reception of NOTIFY?	-->	200 OK	4	P

Table 6.1.3.2-2: Parallel Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	UE sends a PUBLISH request.	-->	PUBLISH		
2	SS sends a 503 Service Unavailable response	<--	503 Service Unavailable		

6.1.3.3 Specific message contents

Table 6.1.3.3-1: REGISTER (step 2, table 6.1.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.1, Condition A1

Table 6.1.3.3-2: 401 Unauthorized for REGISTER (step 3, table 6.1.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.2, Condition A1

Table 6.1.3.3-3: REGISTER (step 4, table 6.1.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.1, Conditions A2 and A32

Table 6.1.3.3-4: 200 OK for REGISTER (step 5, table 6.1.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.3, Condition A2

Table 6.1.3.3-5: SUBSCRIBE for reg-event package (step 6, table 6.1.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.4, Conditions A1 and A7

Table 6.1.3.3-6: 200 OK for SUBSCRIBE (step 7, table 6.1.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.5, Condition A1

Table 6.1.3.3-7: NOTIFY for reg-event package (step 8, table 6.1.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.6, Condition A1

Table 6.1.3.3-8: 200 OK for requests other than REGISTER or SUBSCRIBE (step 9, table 6.1.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.3.1, Conditions A10 and A22

Table 6.1.3.3-9: PUBLISH (step 1, table 6.1.3.2-2)

Derivation Path: TS 34.229-1 [2], Table in subclause A.4.3, Conditions A1 and A5

Table 6.1.3.3-10: 503 Service Unavailable (step 2, table 6.1.3.2-2)

Derivation Path: TS 34.229-1 [2], Table in subclause A.4.2

6.2 Initial Registration Failures / 5GS

6.2.1 Test Purpose (TP)

(1)

```
with { UE having sent unprotected REGISTER request }
ensure that {
  when { UE receiving a 503 (Service Unavailable) response without Retry-After header for the
unprotected REGISTER request sent }
   then { UE waits at most 5 minutes and then sends another unprotected REGISTER request }
            }
```

(2)

```
with { UE having sent an unprotected REGISTER request }
ensure that {
  when { UE receiving a 503 (Service Unavailable) response with Retry-After header for the initial
REGISTER request sent }
   then { UE waits until interval given is up and then sends another unprotected REGISTER request }
            }
```

(3)

```
with { UE having sent unprotected REGISTER request }
ensure that {
  when { UE receiving a 423 (Interval Too Brief) response }
   then { UE sends another unprotect REGISTER request with new expiration interval }
            }
```

6.2.2 Conformance Requirements

[TS 24.229, clause 5.1.1.2.1]:

After a first unsuccessful initial registration attempt, if the Retry-After header field was not present and the initial registration was not performed as a consequence of a failed reregistration, the UE shall not wait more than 5 minutes before attempting a new registration.

[TS 24.229, clause 5.1.1.2.1]:

On receiving a 503 response with a Retry-After header field to the REGISTER request and the Retry-After header field indicates time bigger than the value for timer F as specified in table 7.7.1, the UE:

a) shall mark the currently used P-CSCF address as unavailable for the time indicated by the Retry-After header field;

b) if there is a locally stored P-CSCF address as specified in subclause 5.1.9 which is different than the currently used P-CSCF address and which is not marked as unavailable, may initiate an initial registration as specified in subclause 5.1.1.2 using that P-CSCF; and

c) if there is no locally stored P-CSCF address as specified in subclause 5.1.9 which is different than the currently used P-CSCF address and which is not marked as unavailable, may get a new set of P-CSCF addresses as described in subclause 9.2.1 unless otherwise specified in the access specific annexes (as described in annex B, annex L or annex U) and initiate an initial registration as specified in subclause 5.1.1.2.

NOTE 19: if the Retry-After header field indicates time smaller than the value for timer F as specified in table 7.7.1, the UE continues using the currently used P-CSCF address.

[TS 24.229, clause 5.1.1.2.1]:

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.

6.2.3 Test description

6.2.3.1 Pre-test conditions

System Simulator:

- 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 IMS AKA authentication for the IMPI, according to 3GPP TS 33.203 [16] clause 6.1.
- 1 NR Cell

UE:

- The UE contains either ISIM and USIM applications or only USIM application on UICC.
- The UE is configured to register for IMS after switch on.
- The UE is switched off.

Preamble:

- None

6.2.3.2 Test procedure sequence

Table 6.2.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	The UE is switched on				
2	UE sends an initial registration request.	-->	REGISTER		
3	SS sends 503 Service Unavailable without Retry-After header.	<--	503 Service Unavailable		
4	Check: does the UE not wait more than 5 minutes before attempting a new registration?	-->	REGISTER	1	P
5	SS sends 503 Service Unavailable with Retry-After header set to 10 seconds.	<--	503 Service Unavailable		
6	Check: does the UE send an initial registration request, but no earlier than 10 seconds after step 5?	-->	REGISTER	2	P
7	SS sends 423 Interval Too Brief.	<--	423 Interval Too Brief		
8	Check: does the UE send an initial registration request with an expiration value set to the value provided in Step 7?	-->	REGISTER	3	P
9	SS sends 401 Unauthorized.	<--	401 Unauthorized		
10	UE sends a subsequent registration request.	-->	REGISTER		
11	SS sends 200 OK for REGISTER	<--	200 OK		
	EXCEPTION: In parallel to the events described in steps 12 to 15, the steps specified in Table 6.1.3.2-2 may take place.				
12-15	Steps 5-8 from clause A.2.				

Table 6.2.3.2-2: Parallel Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	UE sends a PUBLISH request.	-->	PUBLISH		
2	SS sends a 503 Service Unavailable response	<--	503 Service Unavailable		

6.2.3.3 Specific message contents

Table 6.2.3.3-1: REGISTER (step 2, table 6.2.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.1, Condition A1

Table 6.2.3.3-2: 503 Service Unavailable (step 3, table 6.2.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.4.2				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Retry-After		not present		

Table 6.2.3.3-3: REGISTER (step 4, table 6.2.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.1, Condition A1				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
CSeq				
value		incremented by one from previous REGISTER		

Table 6.2.3.3-4: 503 Service Unavailable (step 5, table 6.2.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.4.2				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Retry-After				
delta-seconds		10		

Table 6.2.3.3-5: REGISTER (step 6, table 6.2.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.1, Condition A1				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
CSeq				
value		incremented by one from previous REGISTER		

Table 6.2.3.3-6: 423 Interval Too Brief (step 7, table 6.2.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.7				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Min-Expires				
delta-seconds		800000		

Table 6.2.3.3-7: REGISTER (step 8, table 6.2.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.1, Condition A1				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Contact				
expires		800000		
Expires				
delta-seconds		800000 Note: value 800000 is given in at least one of Contact or Expires header.		
CSeq				
value		incremented from previous REGISTER		

Table 6.2.3.3-8: 401 Unauthorized (step 9, table 6.2.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.2, Condition A1

Table 6.2.3.3-9: REGISTER (step 10, table 6.2.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.1, Conditions A2 and A32				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Contact				
expires		800000		
Expires				
delta-seconds		800000 Note: value 800000 is given in at least one of Contact or Expires header.		
CSeq				
value		incremented from previous REGISTER		

Table 6.2.3.3-10: 200 OK (step 11, table 6.2.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.3, Condition A2				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Contact				
expires		800000		

6.3 Re-Registration Scenarios / 5GS

6.3.1 Test Purpose (TP)

(1)

```
with { UE being registered to IMS with expiration interval at 120 seconds }
ensure that {
  when { 60 seconds passed }
    then {UE re-registers }
            }
```

(2)

```
with { UE starting re-registration procedure by sending REGISTER }
ensure that {
  when { UE receives 500 Server Internal Error response }
    then {UE starts initial registration }
            }
```

(3)

```
with { UE being registered to IMS with expiration interval at 360 seconds }
ensure that {
  when { 180 seconds passed }
    then {UE re-registers }
            }
```

(4)

```
with { UE being registered to IMS with expiration interval at 1600 seconds }
ensure that {
  when { 1000 seconds passed }
    then {UE re-registers }
            }
```

(5)

```
with { UE attempting re-registration }
ensure that {
  when { UE receives 423 Interval Too Brief response }
    then {UE sends another re-registration request with given expiration interval }
            }
```

(6)

```
with { UE being registered }
ensure that {
  when { UE receives notification about shortened expiration interval for one of its registered
public user identities }
    then {UE re-registers after half of the shorted expiration interval elapses }
            }
```

6.3.2 Conformance Requirements

[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.

...

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,

...

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.

On receiving a 408 (Request Timeout) response or 500 (Server Internal Error) response or 504 (Server Time-Out) response or 403 (Forbidden) response for a reregistration, the UE shall perform the procedures for initial registration as described in subclause 5.1.1.2.

[TS 24.229, clause 5.1.1.4.1]:

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 expires attribute of 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.

6.3.3 Test description

6.3.3.1 Pre-test conditions

System Simulator:

- 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 IMS AKA authentication for the IMPI, according to 3GPP TS 33.203 [16] clause 6.1.

- 1 NR Cell

UE:

- The UE contains either ISIM and USIM applications or only USIM application on UICC.

- The UE is configured to register for IMS after switch on.

- The UE is switched off.

Preamble:

- None

6.3.3.2 Test procedure sequence

Table 6.3.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	UE is switched on.				
2-9	Steps 1-8 from clause A.2: initial IMS registration happens, with SS giving 120 seconds expiration interval.				
10	UE re-registers 60 seconds later.	-->	REGISTER	1	P
11	SS declines re-registration attempt.	<--	500 Server Internal Error		
12	Step 1 from clause A.2: UE sends initial IMS registration request	-->	REGISTER	2	P
13-19	Steps 2-8 from clause A.2, with SS giving 360 seconds expiration interval.				
20	UE re-registers 180 seconds later.	-->	REGISTER	3	P
21	SS responds with 1600 seconds expiration interval	<--	200 OK		
22	UE re-registers 1000 seconds later	-->	REGISTER	4	P
23	SS responds with 423 Interval Too Brief with Min-Expires value of 800000 seconds	<--	423 Interval Too Brief		
24	UE sends a new another re-registration request using at least 800000 seconds expiration.	-->	REGISTER	5	P
25	SS responds with 200 OK.	<--	200 OK		
26	SS notifies UE about shortened expiration time of 60 seconds for one of the registered public user identities.	<--	NOTIFY		
27	UE responds with 200 OK	-->	200 OK		
28	30 seconds before new expiry time, UE re-registers	-->	REGISTER	6	P
29	SS responds with authentication challenge and security mechanism supported by the network	<--	401 Unauthorized		
30	UE completes security procedures	-->	REGISTER		
31	SS responds with 200 OK	<--	200 OK		

6.3.3.3 Specific message contents

Table 6.3.3.3-1: 200 OK for REGISTER (step 5, Table 6.3.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.3				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Contact				
expires		120		

Table 6.3.3.3-2: REGISTER (step 10, Table 6.3.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.1, Conditions A2, A17, A32				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Security-Client				
spi-c		new SPI number of the inbound SA at the protected client port, shall be different from previously used number		
spi-s		new SPI number of the inbound SA at the protected server port, shall be different from previously used number		
port-c		new protected client port, shall be different from previously used number		
port-s		same value as in the previous REGISTER		
Authorization				RFC 2617 [23]
nonce-count		2		TS 24.229 [7]

Table 6.3.3.3-3: 500 Server Internal Error (step 11, Table 6.3.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.4.7

Table 6.3.3.3-4: 200 OK for REGISTER (step 15, Table 6.3.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.3				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Contact				
expires		360		

Table 6.3.3.3-5: REGISTER (step 20, Table 6.3.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.1, Conditions A2, A17, A32				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Security-Client				
spi-c		new SPI number of the inbound SA at the protected client port, shall be different from previously used numbers		
spi-s		new SPI number of the inbound SA at the protected server port, shall be different from previously used numbers		
port-c		new protected client port, shall be different from previously used numbers		
port-s		same value as in the previous REGISTER		
Authorization				RFC 2617 [23]
nonce-count		2		TS 24.229 [7]

Table 6.3.3.3-6: 200 OK for REGISTER (step 21, Table 6.3.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.3				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Contact				
expires		1600		

Table 6.3.3.3-7: REGISTER (step 22, Table 6.3.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.1, Conditions A2, A17, A32				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Security-Client				
spi-c		new SPI number of the inbound SA at the protected client port, shall be different from previously used numbers		
spi-s		new SPI number of the inbound SA at the protected server port, shall be different from previously used numbers		
port-c		new protected client port, shall be different from previously used numbers		
port-s		same value as in the previous REGISTER		
Authorization				RFC 2617 [23]
nonce-count		3		TS 24.229 [7]

Table 6.3.3.3-8: 423 Interval Too Brief (step 23, Table 6.3.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.7				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Min-Expires				
delta-seconds		800000		

Table 6.3.3.3-9: REGISTER (step 24, Table 6.3.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.1, Conditions A2, A17, A32				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Contact				
expires		800000 or more (Remark: either the Contact header contains such expires parameter or below Expires header is present. If both are present, Expires header is to be ignored)		
Expires				
delta-seconds		800000 or more (Remark: either the Contact header contains above expires parameter or Expires header is present. If both are present, Expires header is to be ignored)		
Authorization				RFC 2617 [23]
nonce-count		4		TS 24.229 [7]

Table 6.3.3.3-10: NOTIFY (step 26, Table 6.3.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.6, Conditions A1, and A3 OR A4				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Message-body				
	A3	*<?xml version="1.0" encoding="UTF-8"?>* *<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"* *version="1" state="partial">* *<registration aor=*" PublicUserIdentity1 (NOTE 1)" *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>*		
	A4	*<?xml version="1.0" encoding="UTF-8"?>* *<reginfo xmlns="urn:ietf:params:xml:ns:reginfo"* *xmlns:gr="urn:ietf:params:xml:ns:gruuinfo" version="1"* *state="partial">* *<registration aor=*" PublicUserIdentity1 (NOTE 1)" *id="a100" state="active">* *<contact id="980" state="active" event="shortened"* *expires="60">* *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>* *<unknown-param name="+sip.instance"> "Instance ID of the UE;" </unknown-param>* *<gr:pub-gruu uri="public GRUU associated to this aor"/>* *<gr:temp-gruu uri="temporary GRUU associated to this aor" first-cseq="CSeq of the REGISTER request that caused the temporary GRUU to assigned for the UE"/>* *</contact>* *</registration>* *</reginfo>*		

Table 6.3.3.3-11: 200 OK for other requests than REGISTER or SUBSCRIBE (step 27, Table 6.3.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.3.1, Conditions A5, A11, A22

Table 6.3.3.3-12: REGISTER (step 28, Table 6.3.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.1, Conditions A2, A17, A32				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Authorization nonce-count		 5		

Table 6.3.3.3-13: 401 Unauthorized (step 29, Table 6.3.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.2, Condition A1				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
WWW-Authenticate nonce		 Base 64 encoding of new RAND and new AUTN (different from the values used in step 3)		RFC 2617 [23] TS 24.229 [7]

Table 6.3.3.3-14: REGISTER (step 30, Table 6.3.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.1, Conditions A2, A17, A32				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Authorization nonce-count		 1		

Table 6.3.3.3-15: 200 OK for REGISTER (step 31, Table 6.3.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.3, Condition A2

6.4 De-Registration Scenarios / 5GS

6.4.1 Test Purpose (TP)

(1)

```
with { UE being registered to IMS }
ensure that {
  when { a REFRESH command happens }
   then { UE waits for the network to de-register the UE from IMS }
            }
```

(2)

```
with { UE being registered to IMS }
ensure that {
  when { UE receiving a NOTIFY request containing de-registration information with contact elements
being "deactivated" }
   then { UE acknowledges de-registration }
            }
```

(3)

```
with { UE being de-registered from IMS by the network with contact elements being "deactivated" }
ensure that {
  when { UE acknowledging de-registration }
   then { UE performs initial registration to IMS }
            }
```

(4)

```
with { UE being registered to IMS }
ensure that {
  when { UE is made to de-register its contact address }
   then { UE performs de-registration from IMS }
            }
```

6.4.2 Conformance Requirements

[TS 24.229, Annex C.4]:

3GPP TS 31.102 [15C] and 3GPP TS 31.103 [15B] 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 [15D]. 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 [15D].

If the UE supports the UICC access to IMS USAT feature defined in 3GPP TS 31.111 [15D] and the $EF_{UICCIARI}$ changes in either the USIM or the ISIM, the UE shall perform the user-initiated reregistration procedure as described in subclause 5.1.1.4 with the new values of the IARI parameter(s) residing on the UICC.

In case of changes to EFs other than the $EF_{UICCIARI}$, 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 5.4.1.5]:

For any registered public user identity, the S-CSCF can deregister:

- all contact addresses bound to the indicated public user identity (i.e. deregister the respective public user identity);
- some contact addresses bound to the indicated public user identity;
- a particular contact address bound to the indicated public user identity; or
- one or more registration flows and the associated contact address bound to the indicated public user identity, when the UE supports multiple registration procedure;

by sending a single NOTIFY request.

...

When a network-initiated deregistration event occurs for one or more public user identities that are bound either to one or more contact addresses or registration flows and the associated contact addresses (if the multiple registration mechanism is used), the S-CSCF shall send a NOTIFY request to all subscribers that have subscribed to the respective reg event package. For each NOTIFY request, the S-CSCF shall:

1) set the Request-URI and Route header field to the saved route information during subscription;

2) set the Event header field to the "reg" value;

3) in the body of the NOTIFY request, include as many <registration> elements as many public user identities the S-CSCF is aware of the user owns;

4) set the aor attribute within each <registration> element to one public user identity:

   a) set the <uri> sub-element inside each <contact> sub-element of each <registration> element to the respective contact address provided by the UE;

   b) if the public user identity:

      i) has been deregistered (i.e. all contact addresses and all registration flows and associated contact addresses bound to the indicated public user identity are removed) then:

         - set the state attribute within the <registration> element to "terminated";

         - set the state attribute within each <contact> element belonging to this UE to "terminated"; and

         - set the event attribute within each <contact> element belonging to this UE to either "unregistered", or "deactivated" if the S-CSCF expects the UE to reregister or "rejected" if the S-CSCF does not expect the UE to reregister; or

...
When sending a final NOTIFY request with all <registration> element(s) having their state attribute set to "terminated" (i.e. all public user identities have been deregistered or expired), the S-CSCF shall also terminate the subscription to the registration event package by setting the Subscription-State header field to the value of "terminated".

[TS 24.229, clause 5.1.1.7]:

Upon receipt of a NOTIFY request, on any dialog which was generated during the 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:

1) the state attribute within the <registration> element set to "terminated", and within each <contact> element belonging to this UE, the state attribute set to "terminated" and the event attribute set either to "unregistered", or "rejected", or "deactivated", the UE shall remove all registration details relating to the respective public user identity (i.e. consider the public user identity indicated in the aor attribute of the <registration> element as deregistered); or

...

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 all security associations or TLS sessions towards the P-CSCF either:

- if all <registration> element(s) have their state attribute set to "terminated" (i.e. all public user identities are deregistered) and the Subscription-State header field 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".

When all UE's public user identities are registered via a single P-CSCF and the subscription dialog to the reg event package of the UE is set via the respective P-CSCF, the UE shall delete these security associations or TLS sessions towards the respective P-CSCF when all public user identities have been deregistered and after the server transaction (as defined in RFC 3261 [26]) pertaining to the received NOTIFY request terminates.

NOTE 3: Deleting a security association or TLS session is an internal procedure of the UE and does not involve any SIP procedures.

NOTE 4: If all the public user identities (i.e. <contact> elements) registered by this UE are deregistered and the security associations or TLS sessions have been removed, the UE considers the subscription to the reg event package terminated since the NOTIFY request was received with Subscription-State header field containing the value of "terminated".

[TS 24.229, clause 5.1.1.6.1]:

For any public user identity that the UE has previously registered, the UE can deregister via a single registration procedure:

- all contact addresses bound to the indicated public user identity;
- some contact addresses bound to the indicated public user identity;
- a particular contact address bound to the indicated public user identity; or
- when the UE supports multiple registrations (i.e. the "outbound" option tag is included in the Supported header field) one or more flows bound to the indicated public user identity.

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 [19], 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 or the flow 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 or one of its flows, the UE shall populate the header fields as follows:

a) a From header field set to the SIP URI that contains:

   1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else

   2) the public user identity to be deregistered;

b) a To header field set to the SIP URI that contains:

   1) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, the main URI of the UE; else

   2) 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:

1) if the UE is removing the binding between the public user identity indicated in the To header field, (together with the associated implicitly registered public user identities), and the contact address indicated in the Contact header field; and

   - if the UE supports GRUU, or multiple registrations (i.e. the "outbound" option tag is included in the Supported header field), or has an IMEI available, or has an MEID available, the Contact header field also contains the "+sip.instance" header field parameter. Only the IMEI shall be used for generating an instance ID for a multi-mode UE that supports both 3GPP and 3GPP2 defined radio access networks;

   - if the UE supports multiple registrations (i.e. the "outbound" option tag is included in the Supported header field), the Contact header field does not contain the "reg-id" header field parameter;

   - if the UE does not supports GRUU and does not support multiple registrations (i.e. the "outbound" option tag is not included in the Supported header field), and does not have an IMEI available, and does not have an MEID available, the Contact header field does not contain either the "+sip.instance" header field parameter or the "reg-id" header field parameter;

NOTE 1: Since the contact address is deregistered, if there are any flows that were previously registered with the respective contact address, all flows terminating at the respective contact address are removed.

2) if the UE is removing the binding between the public user identity indicated in the To header field, (together with the associated implicitly registered public user identities) and one of its flows, the Contact header field contains the "+sip.instance" header field parameter and the "reg-id" header field parameter that identifies the flow; and

NOTE 2: The requirement placed on the UE to include an instance ID based on the IMEI when the UE does not support GRUU and does not support multiple registrations does not imply any additional requirements on the network.

3) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Contact URI without a user portion and containing the "bnc" URI parameter;

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);

h) a Security-Client header field to announce the media plane security mechanisms the UE supports, if any;

NOTE 3: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

i) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Require header field containing the option-tag "gin"; and

j) if the UE supports RFC 6140 [191] and performs the functions of an external attached network, for the registration of bulk number contacts the UE shall include a Proxy-Require header field containing the option-tag "gin".

For a public user identity that the UE has registered with multiple contact addresses or multiple flows (e.g. via different P-CSCFs), the UE shall also be able to deregister multiple contact addresses or multiple flows, bound to its public user identity, via single deregistration procedure as specified in RFC 3261 [26]. 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 field is populated as specified above in bullets a) through i).

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". The UE shall not include the "instance-id" feature tag and the "reg-id" header field parameter in the Contact header field in the REGISTER request.

NOTE 4: All entities subscribed to the reg event package of the user will be informed 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 labelled with the "mediasec" header field parameter specified in subclause 7.2A.7 and received in the Security-Server header field, if any.

NOTE 5: The "mediasec" header field parameter indicates that security mechanisms are specific to the media plane.

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 [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.

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.

6.4.3 Test description

6.4.3.1 Pre-test conditions

System Simulator:

- 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 IMS AKA authentication for the IMPI, according to 3GPP TS 33.203 [16] clause 6.1.
- 1 NR Cell

UE:

- The UE contains either ISIM and USIM applications or only USIM application on UICC.
- The UE is configured to register for IMS after switch on.
- The UE is switched off.

Preamble:

- None

6.4.3.2 Test procedure sequence

Table 6.4.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	UE is switched on.				
2-9	Steps 1-8 from clause A.2: initial IMS registration happens.				
10	The UICC is made to send a REFRESH command to the UE indicating that contents of ISIM has been updated.		REFRESH		
11	The SS waits for 5 seconds.				
12	Check: does the UE send a REGISTER request			1	F
13	SS de-registers the UE's contact address.	<--	NOTIFY		
14	UE acknowledges.	-->	200 OK	2	P
15-22	Steps 1-8 from clause A.2: initial IMS registration happens. For the Request-URI, the UE uses the new value of home domain and/or IMS identities name as provided by ISIM after the update in step 10.			3	P
23	UE is made to de-register its contact address.				
24-29	Steps 0A-2 defined in TS 34.229-1 [2] cl C.30			4	P

6.4.3.3 Specific message contents

Table 6.4.3.3-0: REFRESH (step 10, table 6.4.3.2-1)

Derivation Path: TS 31.111, subclause 6.4.7

Table 6.4.3.3-1: NOTIFY (step 13, Table 6.4.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.6, Conditions A1 AND ((A3 AND A6) OR (A4 AND A6))

Table 6.4.3.3-2: 200 OK for other requests than REGISTER or SUBSCRIBE (step 14, Table 6.4.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.3.1, Conditions A5, A11, A22

6.5 Refresh for ISIM parameters / 5GS

6.5.1 Test Purpose (TP)

(1)

```
with { UE being registered to IMS }
ensure that {
  when { UE receives indication that contents of USIM/ISIM has been updated }
    then { UE does not de-register from IMS }
           }
```

(2)

```
with { UE waiting for network-initiated de-registration }
ensure that {
  when { UE receives NOTIFY request for reg event }
    then { UE responds with a valid 200 OK response and initiates new IMS registration }
           }
```

6.5.2 Conformance Requirements

[TS 24.229 Annex C.4]:

3GPP TS 31.102 [15C] and 3GPP TS 31.103 [15B] 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 [15D]. 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 [15D].

If the UE supports the UICC access to IMS USAT feature defined in 3GPP TS 31.111 [15D] and the $EF_{UICCIARI}$ changes in either the USIM or the ISIM, the UE shall perform the user-initiated reregistration procedure as described in subclause 5.1.1.4 with the new values of the IARI parameter(s) residing on the UICC.

In case of changes to EFs other than the $EF_{UICCIARI}$, 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 the 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:

1) the state attribute within the <registration> element set to "terminated", and within each <contact> element belonging to this UE, the state attribute set to "terminated" and the event attribute set either to "unregistered", or "rejected", or "deactivated", the UE shall remove all registration details relating to the respective public user identity (i.e. consider the public user identity indicated in the aor attribute of the <registration> element as deregistered); or

2) the state attribute within the <registration> element set to "active", and within a given <contact> element belonging to this UE, the state attribute set to "terminated", and the associated event attribute set either to "unregistered", or "rejected" or "deactivated", the UE shall consider the binding between the public user identity and either the contact address or the registration flow and the associated contact address (if the multiple registration mechanism is used) indicated in the respective <contact> element as removed. The UE shall consider its public user identity as deregistered when all bindings between the respective public user identity and all contact addresses and all registration flow and the associated contact address (if the multiple registration mechanism is used) belonging to this UE are removed.

NOTE 1: When multiple registration mechanism is used to register a public user identity and bind it to a registration flow and the associated contact address, there will be one <contact> element for each registration flow and the associated contact address.

NOTE 2: If the state attribute within the <registration> element is set to "active" and the <contact> element belonging to this UE is set to "active", the UE will consider that the binding between the public user identity and either the respective contact address or the registration flow and the associated contact address as left unchanged.

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.

Reference(s)

3GPP TS 24.229 [7] annex C.4 and clause 5.1.1.7.

6.5.3 Test description

6.5.3.1 Pre-test conditions

System Simulator:

- 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 able to perform AKAv1-MD5 authentication algorithm for that IMPI, according to 3GPP TS 33.203 [16] clause 6.1 and RFC 3310 [15].
- SS is listening to SIP default port 5060 for both UDP and TCP protocols.
- 1 NR Cell

UE:

- UE contains either ISIM and USIM applications or only USIM application on UICC.
- UE is registered to IMS services.
- The Request-URI of SIP REGISTER request sent by the UE contained the old home domain name and IMS identities as found from ISIM.

Preamble:

- None.

6.5.3.2 Test procedure sequence

Table 6.5.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	The UICC is made to send a REFRESH command to the UE indicating that contents of ISIM has been updated.		REFRESH		
2	Check: does the UE de-register from IMS?			1	F
3	10 seconds after 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"	<--	NOTIFY		
4	Check: does the UE respond the NOTIFY with 200 OK?	-->	200 OK	2	P
5	Check: does the UE initiate 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.	-->	REGISTER	2	P
6-12	Continue with Annex A.2 step 2-8 in order to get the UE in a stable registered state.	-			

6.5.3.3 Specific message contents

Table 6.5.3.3-1: REFRESH (step 1, table 6.5.3.2-1)

Derivation Path: TS 31.111, subclause 6.4.7

Table 6.5.3.3-2: NOTIFY for reg-event package (step 3, table 6.5.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.6, Conditions A1 AND ((A3 AND A6) OR (A4 AND A6))

Table 6.5.3.3-3: 200 OK for requests other than REGISTER or SUBSCRIBE (step 4, table 6.5.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.3.1, Conditions A5, A11 and A22

Table 6.5.3.3-4: REGISTER (step 5, table 6.5.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.1, Condition A1

6.6 Re-Registration after capability update / 5GS

6.6.1 Test Purpose (TP)

(1)

```
with { UE being registered to IMS }
ensure that {
  when { UE is made to update its capabilities }
    then { UE re-registers }
           }
```

6.6.2 Conformance Requirements

[TS 24.229, clause 5.1.1.4.1]:

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 [62] 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.

6.6.3 Test description

6.6.3.1 Pre-test conditions

System Simulator:

- SS is configured 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 [16] clause 6.1 and RFC 3310 [15].
- SS is listening to SIP default port 5060 for both UDP and TCP protocols.
- 1 NR Cell

UE:

- 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 A.2 up to the last step.
- UE is able to be made change its capabilities, manifested through a specific instance which is setting the AT Command +CASIMS (Availability for SMS using IMS, defined in 3GPP TS 27.007 [22] 8.72) to 0.

Preamble:

- None.

6.6.3.2 Test procedure sequence

Table 6.6.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	Turning off the UE's SMS over IMS capability through AT command +CASIMS (3GPP TS 27.007 clause 8.72) set to 0.				
2	Check: does the UE initiate a re-registration procedure, and indicating the changed capabilities in the REGISTER message?	-->	REGISTER	1	P
3	SS responds 401 Unauthorized	<--	401 Unauthorized		
4	UE sends a subsequent registration request	-->	REGISTER		
5	SS responds with 200 OK for REGISTER	<--	200 OK		

6.6.3.3 Specific message contents

Table 6.6.3.3-1: REGISTER (step 2, table 6.6.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.1, Condition A2, A17 and A32				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Contact				
feature-param		does not contain "+g.3gpp.smsip"		
Authorization				
nonce-count		2		

Table 6.6.3.3-2: 401 Unauthorized for REGISTER (step 3, table 6.6.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.2, Condition A1				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
WWW-Authenticate				RFC 2617 [23]
nonce		Base 64 encoding of new RAND and new AUTN (different from the values used in initial registration)		TS 24.229 [7]

Table 6.6.3.3-3: REGISTER (step 4, table 6.6.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.1, Conditions A2, A17 and A32				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Authorization				
nonce-count		1 (UE received new nonce at step 3)		

Table 6.6.3.3-4: 200 OK for REGISTER (step 5, table 6.6.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.3, Condition A2

6.7 Authentication / MAC Parameter Invalid / Only two consecutive invalid challenges / 5GS

6.7.1 Test Purpose (TP)

(1)

```
with { UE starting registration procedure }
ensure that {
  when { UE receiving invalid MAC parameter }
    then { UE sends another REGISTER request without challenge response AUTS and populates a new
Security-Client header }
            }
```

(2)

```
with { UE having responded to invalid MAC parameter }
ensure that {
  when { UE receives another invalid MAC parameter }
    then { UE sends another REGISTER request without challenge response AUTS and populates a new
Security-Client header }
            }
```

(3)

```
with { UE having responded to invalid MAC parameter twice }
ensure that {
  when { UE receives an invalid MAC parameter for a third time }
    then { UE does not send another REGISTER request }
            }
```

6.7.2 Conformance Requirements

[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;

…

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 [16]);
- 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. These parameters shall contain new values for spi_uc, spi_us and port_uc; and
- not create a temporary set of security associations.

[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 receiving two consecutive invalid challenges. The UE may attempt to register with the network again after an implementation specific time.

Reference(s)

3GPP TS 24.229 [7] clause 5.1.1.5.3 and clause 5.1.1.5.12.

6.7.3 Test description

6.7.3.1 Pre-test conditions

System Simulator:

- 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 [16] clause 6.1 and RFC 3310 [15].
- SS is listening to SIP default port 5060 for both UDP and TCP protocols.
- 1 NR Cell

UE:

- UE contains either ISIM and USIM applications or only USIM application on UICC.
- The UE is configured to register for IMS after switch on.
- The UE is switched off.

Preamble:

- None.

6.7.3.2 Test procedure sequence

Table 6.7.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	The UE is switched on.				
2	UE sends initial registration for IMS services.	-->	REGISTER		
3	SS responds with an invalid AKAv1-MD5 authentication challenge with an invalid MAC value.	<--	401 Unauthorized		
4	Check: does the UE send a 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	-->	REGISTER	1	P
5	SS responds with an invalid AKAv1-MD5 authentication challenge with an invalid MAC value.	<--	401 Unauthorized		
6	Check: does the UE send another 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	-->	REGISTER	2	P
7	SS responds with an invalid AKAv1-MD5 authentication challenge with an invalid MAC value.	<--	401 Unauthorized		
8	Check: does the UE send another REGISTER: - The SS waits for 10 seconds to see whether there would be another REGISTER.			3	F

6.7.3.3 Specific message contents

Table 6.7.3.3-1: REGISTER (step 2, table 6.7.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.1, Condition A1

Table 6.7.3.3-2: 401 Unauthorized for REGISTER (step 3/5/7, table 6.7.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.2, Condition A1				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
WWW-Authenticate				
nonce		Base 64 encoding of RAND and AUTN, generated using invalid MAC value		

Table 6.7.3.3-3: REGISTER (step 4/6, table 6.7.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.1, Condition A1				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
CSeq				
value		must be incremented from previous REGISTER		
Call-ID				
callid		same value as in REGISTER at Step 2		
Authorization				
response		present, but empty		
auts		not present		
Security-Client				
spi-c		new SPI number of the inbound SA at the protected client port, shall be different from previously used number(s)		
spi-s		new SPI number of the inbound SA at the protected server port, shall be different from previously used number(s)		
port-c		new protected client port, shall be different from previously used number(s)		

6.8 Authentication / Security-Server missing / SQN out of range / 5GS

6.8.1 Test Purpose (TP)

(1)

```
with { UE starting registration procedure }
ensure that {
  when { UE receiving a challenge response without Security-Server header }
    then { UE abandons the authentication procedure and sends a new REGISTER request with new Call-
           ID }
            }
```

(2)

```
with { UE having sent a new initial REGISTER request }
ensure that {
  when { UE receiving a challenge response with SQN out of range }
    then { UE sends another REGISTER request with challenge response AUTS and populates a new
Security-Client header }
            }
```

6.8.2 Conformance Requirements

[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 [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 is deemed to be invalid then the UE shall behave as defined in subclause 5.1.1.5.3.

[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: 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. These parameters shall contain new values for spi_uc, spi_us and port_uc; and
- not create a temporary set of security associations.

Reference(s)

3GPP TS 24.229 [7] clause 5.1.1.5.1 and clause 5.1.1.5.3.

6.8.3 Test description

6.8.3.1 Pre-test conditions

System Simulator:

- 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 [16] clause 6.1 and RFC 3310 [15].
- SS is listening to SIP default port 5060 for both UDP and TCP protocols.
- 1 NR Cell

UE:

- UE contains either ISIM and USIM applications or only USIM application on UICC.
- The UE is configured to register for IMS after switch on.
- The UE is switched off.

Preamble:

- None.

6.8.3.2 Test procedure sequence

Table 6.8.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	The UE is switched on.				
2	UE sends initial registration for IMS services.	-->	REGISTER		
3	SS responds challenge response without Security-Server header.	<--	401 Unauthorized		
4	Check: does the UE sends a new REGISTER request with new Call-ID	-->	REGISTER	1	P
5	SS responds with an invalid AKAv1-MD5 authentication challenge with SQN out of range.	<--	401 Unauthorized		
6	Check: does the UE send another 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.	-->	REGISTER	2	P
7-13	Continue with Annex A.2 step 2-8 in order to get the UE in a stable registered state.	-			

6.8.3.3 Specific message contents

Table 6.8.3.3-1: REGISTER (step 2, table 6.8.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.1, Condition A1

Table 6.8.3.3-2: 401 Unauthorized for REGISTER (step 3, table 6.8.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.2, Condition A1				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Security-Server		not present.		

Table 6.8.3.3-3: REGISTER (step 4, table 6.8.3.2-1)

Derivation path: TS 34.229-1 [2], Table in subclause A.1.1, Condition A1 and A32				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Call-ID callid		Value differs from the one sent in in Step 2 of table 6.8.3.2-1.		

Table 6.8.3.3-4: 401 Unauthorized for REGISTER (step 5, table 6.8.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.2, Condition A1				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
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 ISIM/USIM, see TS 34.108 clause 8.1.2.2.		

Table 6.8.3.3-5: REGISTER (step 6, table 6.8.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.1, Conditions A1				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
CSeq				
value		must be incremented from previous REGISTER		
Call-ID				
callid		same value as in REGISTER at Step 4		
Authorization				
nonce		same as in previous 401 UNAUTHORIZED message		
opaque		same as in previous 401 UNAUTHORIZED message		
auts		any value		
Security-Client				
spi-c		new SPI number of the inbound SA at the protected client port, shall be different from previously used number		
spi-s		new SPI number of the inbound SA at the protected server port, shall be different from previously used number		
port-c		new protected client port, shall be different from previously used number		

6.9 Subscription / 503 Service Unavailable / 5GS

6.9.1 Test Purpose (TP)

(1)

```
with { UE subscribing to reg event }
ensure that {
  when { UE receives 503 Service unavailable containing a Retry-After header field }
    then { UE does not reattempt the request for the indicated time period }
           }
```

6.9.2 Conformance Requirements

[TS 24.229 clause 5.1.2.2]:

If the UE receives a 503 (Service Unavailable) response to an initial SUBSCRIBE request containing a Retry-After header field, then the UE shall not automatically reattempt the request until after the period indicated by the Retry-After header field contents.

6.9.3 Test description

6.9.3.1 Pre-test conditions

System Simulator:

- 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 is listening to SIP default port 5060 for both UDP and TCP protocols.
- 1 NR Cell

UE:

- UE contains either ISIM and USIM applications or only USIM application on UICC.
- The UE is configured to register for IMS after switch on.
- The UE is switched off.

Preamble:

- None.

6.9.3.2 Test procedure sequence

Table 6.9.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	The UE is switched on.				
2-5	Steps 1-4 of Annex A.2 happen.				
6	UE subscribes to its registration event package.	-->	SUBSCRIBE		
7	SS responds with 503 response containing a Retry-After header with period set to T=128s.	<--	503 Service Unavailable		
8	Check: does the SS receive the UE's re-attempt of SUBSCRIBE within the Time T=128s?			1	F
9	UE reattempts to subscribe to its registration event package.	-->	SUBSCRIBE		
10-12	Continue with Annex A.2 step 6-8 in order to get the UE in a stable registered state.	-			

6.9.3.3 Specific message contents

Table 6.9.3.3-1: SUBSCRIBE for reg-event package (step 6, table 6.9.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.4, Conditions A1 and A7

Table 6.9.3.3-2: 503 Service Unavailable (step 7, table 6.9.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.4.2				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Retry-After				RFC 3261 [6]
period		128		

Table 6.9.3.3-3: SUBSCRIBE for reg-event package (step 9, table 6.9.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.1.4, Conditions A1 and A7				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Call-ID				RFC 3261 [6]
callid		value different from the previous SUBSCRIBE request		

7. Call Control

7.1 to 7.3 FFS

7.4 MTSI MO Voice Call with preconditions at both originating and terminating UE / 5GS

7.4.1 Test Purpose (TP)

(1)

```
with { UE being registered to IMS and configured to use preconditions }
ensure that {
  when { UE is being made to initiate a voice call }
   then { UE sends INVITE for voice call with preconditions }
            }
```

(2)

```
with { UE having sent INVITE with preconditions }
ensure that {
  when { UE receives 100 Trying followed by 183 Session Progress }
   then { UE sends PRACK for 183 Session Progress }
            }
```

(3)

```
with { UE having sent PRACK }
ensure that {
  when { UE receives 200 OK for PRACK and resources are available }
   then { UE sends UPDATE }
            }
```

(4)

```
with { UE having sent UPDATE }
ensure that {
  when { UE receives 200 OK for UPDATE followed by 180 Ringing sent reliably }
   then { UE sends PRACK for 180 Ringing }
            }
```

(5)

```
with { UE having sent PRACK for 180 Ringing }
ensure that {
  when { UE receives 200 OK for PRACK followed by 200 OK for INVITE }
   then { UE sends ACK }
            }
```

7.4.2 Conformance Requirements

Editor's Note: Conformance Requirements should be revisited in order to trim them down to the necessary.

[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 re-uses a previously registered contact address, the UE shall remove any parameters dedicated to registration from the Contact header field (e.g. "expires").

When the UE sends any request, the UE shall use either a given contact address that has been previously registered or a registration flow and the associated contact address (if the multiple registration mechanism is used) and 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;

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; and

c) if a nonce value for proxy authentication is stored for the related registration or registration flow (if the multiple registration mechanism is used), insert a Proxy-Authorization header field containing a challenge response, constructed using the stored nonce value for proxy authentication for the same registration or registration flow (if the multiple registration mechanism is used), "cnonce", "qop", and "nonce-count" header field parameters as specified in RFC 2617 [21];

- if SIP digest with 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 protected server port;

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

c) if a nonce value for proxy authentication is stored for the related registration or registration flow (if the multiple registration mechanism is used), insert a Proxy-Authorization header field containing a challenge response, constructed using the stored nonce value for proxy authentication for the same registration or registration flow (if the multiple registration mechanism is used), "cnonce", "qop", and "nonce-count" header field parameters as specified in RFC 2617 [21];

- if NASS-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 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 SIP digest without TLS is used, the UE shall not include RFC 3329 [48] header field s in any SIP messages.

When SIP digest is in use, upon receiving a 407 (Proxy Authentication Required) response to an initial request, the originating UE shall:

- extract the digest-challenge parameters as indicated in RFC 2617 [21] from the Proxy-Authenticate header field;

- if the contained nonce value is associated to the realm used for the related REGISTER request authentication, store the contained nonce as a nonce value for proxy authentication associated to the same registration or registration flow (if the multiple registration mechanism is used) and shall delete any other previously stored nonce value for proxy authentication for this registration or registration flow;

- calculate the response as described in RFC 2617 [21] using the stored nonce value for proxy authentication associated to the same registration or registration flow (if the multiple registration mechanism is used); and

- send a new request containing a Proxy-Authorization header field in which the header field parameters are populated as defined in RFC 2617 [21] using the calculated response.

Where a security association or TLS session exists, the UE shall discard any SIP response that is not protected by the security association or TLS session and is received from the P-CSCF outside of the registration and authentication procedures. The requirements on the UE within the registration and authentication procedures are defined in subclause 5.1.1.

For a UE performing the functions of an external attached network operating in static mode, authentication can take place without a registration based on TLS client certificate. Before any originating or terminating procedures can take place between the UE performing the functions of an external attached operating in static mode and the P-CSCF or between the UE performing the functions of an external attached network operating in static mode and the IBCF of the IMS network, for security and authentication between the UE performing the functions of an external attached network operating in static mode and the IMS network, the UE performing the functions of an external attached network operating in static mode shall use the TLS procedures according to 3GPP TS 33.310 [19D] using certificates.

In accordance with RFC 3325 [34] the UE may insert a P-Preferred-Identity header field in any initial request for a dialog or request for a standalone transaction as a hint for creation of an asserted identity (contained in the P-Asserted-Identity header field) within the IM CN subsystem.

NOTE 1: Since the S-CSCF uses the P-Asserted-Identity header field when checking whether the UE originating request matches the initial filter criteria, the P-Preferred-Identity header field inserted by the UE determines which services and applications are invoked.

When sending any initial request for a dialog or request for a standalone transaction using either a given contact address that has been previously registered or a registration flow and the associated contact address (if the multiple registration mechanism is used), the UE may include any of the following in the P-Preferred-Identity header field:

- a public user identity which has been registered by the user with the respective contact address;
- an implicitly registered public user identity returned in a registration-state event package of a NOTIFY request whose <uri> sub-element inside the <contact> sub-element of the <registration> element is the same as the contact address being used for this request and was not subsequently deregistered or that has not expired; or
- any other public user identity which the user has assumed by mechanisms outside the scope of this specification to have a current registration.

NOTE 2: The temporary public user identity specified in subclause 5.1.1.1 is not a public user identity suitable for use in the P-Preferred-Identity header field.

NOTE 3: Procedures in the network require international public telecommunication numbers when telephone numbers are used in P-Preferred-Identity header field.

NOTE 4: 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.

Where privacy is required, in any initial request for a dialog or request for a standalone transaction, the UE shall set a display-name of the From header field to "Anonymous" as specified in RFC 3261 [26] and set an addr-spec of the From header field to Anonymous User Identity as specified in 3GPP TS 23.003 [3].

NOTE 5: The contents of the From header field are not necessarily modified by the network based on any privacy specified by the user either within the UE indication of privacy or by network subscription or network policy. Therefore the user should include the value "Anonymous" whenever privacy is explicitly required. As the user can well have privacy requirements, terminal manufacturers should not automatically derive and include values in this header field from the public user identity or other values stored in or derived from the UICC. Where the user has not expressed a preference in the configuration of the terminal implementation, the implementation should assume that privacy is required. Users that require to identify themselves, and are making calls to SIP destinations beyond the IM CN subsystem, where the destination does not implement RFC 3325 [34], will need to include a value in the From header field other than Anonymous.

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). Including the "+sip.instance" header field parameter containing an IMEI URN does not violate RFC 7254 [153] even when the UE requests privacy using RFC 3323 [33].

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 [93]; 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 [93];

   - otherwise, a SIP URI containing the contact address of the UE that has been previously registered without any contact parameters dedicated to registration procedure;

   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 [92];

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 [56B], 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 [56B], 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 within an existing dialog, and the request includes a Contact header field, then the UE should insert the previously used Contact header field.

If the UE support multiple registrations as specified in RFC 5626 [92], the UE should include option-tag "outbound" in the Supported header field.

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 RFC 6050 [121]. If a list of network supported ICSI values was received as specified in 3GPP TS 24.167 [8G], 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. The UE may remove one or more subclasses from an ICSI when including it in an Accept-Contact header field provided that the included ICSI corresponds to an IMS communication service.

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 [56B].

NOTE 10: RFC 3841 [56B] 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 [7].

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.

The UE can indicate privacy of the P-Asserted-Identity that will be generated by the P-CSCF in accordance with RFC 3323 [33], and the additional requirements contained within RFC 3325 [34].

If resource priority in accordance with RFC 4412 [116] is required for a dialog, then the UE shall include the Resource-Priority header field in all requests associated with that dialog.

NOTE 12: The case where the UE is unaware of the requirement for resource priority because the user requested the capability as part of the dialstring falls outside the scope of this requirement. Such cases can exist and will need to be dealt with by an appropriate functional entity (e.g. P-CSCF) to process the dialstring. For certain national implementations, signalling of a Resource-Priority header field to or from a UE is not required.

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 CANCEL requests) or response (except CANCEL responses) within a dialog or any request for a standalone method (see subclause 7.2A.4). Insertion of the P-Access-Network-Info header field into the ACK request is optional.

NOTE 13: 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).

NOTE 14: The value of the P-Access-Network-Info header field could be stale if the point of attachment of the UE with the network changes before the message is received by the network.

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 acquired at the time of the P-CSCF discovery procedures which was used in registration of the contact address (or registration flow); and

NOTE 15: If the UE is provisioned with or receives a FQDN at the time of the P-CSCF discovery procedures, the FQDN is resolved to an IP address at the time of the P-CSCF discovery procedures.

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.

NOTE 16: When the UE registers multiple contact addresses, there will be a list of Service-Route headers for each contact address. When sending a request using a given contact address and the associated security associations or TLS session, the UE will use the corresponding list of Service-Route headers to construct a list of Route headers.

The UE may indicate that proxies should not fork the request by including a "no-fork" directive within the Request-Disposition header field in the request as described in RFC 3841 [56B].

If a request is for a new dialog or standalone transaction, and the request matches a trigger for starting logging of SIP signalling, as described in RFC 8497 [140] and configured in the trace management object defined in 3GPP TS 24.323 [8K], the UE shall:

- start to log SIP signalling for this dialog; and

- in any requests or responses sent on this dialog, append a "logme" header field parameter to the SIP Session-ID header field.

If a request or response is sent on a dialog for which logging of signalling is in progress, the UE shall check whether a trigger for stopping logging of SIP signalling has occurred, as described in RFC 8497 [140] and configured in the trace management object defined in 3GPP TS 24.323 [8K].

a) If a stop trigger event has occurred, the UE shall stop logging of signalling; or

b) if a stop trigger event has not occurred, the UE shall:

   - in any requests or responses sent on this dialog, append a "logme" header field parameter to the SIP Session-ID header field; and

   - log the request.

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], the UE procedures in subclause 5.1.6.10 apply.

If the UE receives a 3xx response containing a Contact header field:

1) if the 3xx response is 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 of the Path header field value received during registration and the response contains 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 7.6.2) then the UE shall select a domain in accordance with the conventions and rules specified in 3GPP TS 22.101 [1A] and 3GPP TS 23.167 [4B], and:

   - if the CS domain is selected, the UE behaviour is defined in subclause 7.1.2 of 3GPP TS 23.167 [4B] and, where appropriate, in the access technology specific annex;

   - if the IM CN subsystem is selected, the UE shall apply the procedures in subclause 5.1.6 with the exception of selecting a domain for the emergency call attempt; and

2) if the response is:

   - not a 380 (Alternative Service) response; or

   - a 380 (Alternative Service) response, and the response:

      i. does not contain 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 7.6.2); or

      ii. does contain 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 7.6.2), and the response;

I) does not contain a P-Asserted-Identity header field; or

II) does contain a P-Asserted-Identity header field with a value not equal to the value of the last entry of the Path header field value received during registration;

the UE should not automatically recurse on the Contact header field without first indicating the identity of the user to which a request will be sent and obtaining authorisation of the served user.

NOTE 17: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF. If there are multiple registration flows associated with the registration, then the UE has received from the P-CSCF during registration multiple sets of Path header field values. The last entry of the Path header field value corresponding to the flow on which the 380 (Alternative Service) response was received is checked.

NOTE 18: A UE can still automatically recurse on 3xx responses as part of a service if the nature of the service enables the UE to identify 3xx responses as having originated from the home network and networks trusted by the home network and the nature of the service ensures that the charging for the requests sent as a result of the 3xx response is correlated with the original request.

NOTE 19: Automatically recursing on untrusted 3xx responses opens up the UE to being redirected to premium rate URIs without the user's consent.

The UE performing the functions of an external attached network operating in static mode shall send all requests using the already established TLS session as described in this subclause.

A UE supporting RFC 4028 [58], when it receives a 422 (Session Interval Too Small) to an INVITE request where the response contains a Min-SE header field, shall retry the request in accordance with RFC 4028 [58] subclause 7.4.

[TS 24.229, clause 5.1.2A.1.2]:

The UE may include a SIP URI complying with RFC 3261 [26], a tel URI complying with RFC 3966 [22], a pres URI complying with RFC 3859 [179], an im URI complying with RFC 3860 [180] or a mailto URI complying with RFC 2368 [181].

NOTE: This version of the document does not specify how the UE determines the host part of the SIP URI.

The UE may use non-international formats of E.164 numbers or non-E.164 numbers, including geo-local numbers and home-local numbers and other local numbers (e.g. private number), in the Request-URI.

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, see subclauses 5.1.2A.1.3 and 5.1.2A.1.4.

[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 network domain name in accordance with RFC 3966 [22].

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 [22] 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 network domain name prefixed by the "geo-local." string according to RFC 3966 [22] 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 or the UE is unable to determine the type of the dialled number, the UE shall include a "phone-context" tel URI parameter set according to RFC 3966 [22], e.g. if private numbers are used a domain name to which the private addressing plan is associated. The "phone-context" value used in the case of other local numbers shall be different from "phone-context" values used with geo-local numbers and home-local numbers.

NOTE 1: The "phone-context" tel URI parameter value can be entered or selected by the subscriber, or can be a "pre-configured" value (e.g. using OMA-DM with the management object specified in 3GPP TS 24.167 [8G]) inserted by the UE.

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 in absence of matching UE configuration in subclause 5.1.2A.1.5A, 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]:

Where multiple domains exist for initiating a call/session, before sending an initial INVITE request, the UE shall perform access domain selection in accordance with the appropriate specification for the IP-CAN in use, taking into account the media to be requested. Access domain selection allows the policy of the network operator to be taken into account before the initial INVITE request is sent. Access dependent aspects of access domain selection are defined in the access technology specific annexes for each access technology.

Upon generating an initial INVITE request, the UE shall include the Accept header field with "application/sdp", the MIME type associated with the 3GPP IM CN subsystem XML body (see subclause 7.6.1) and any other MIME type the UE is willing and capable to accept.

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 [30] as updated by RFC 4032 [64].

The preconditions mechanism should be supported by the originating UE.

If the precondition mechanism is disabled as specified in subclause 5.1.5A, the UE shall not use the precondition mechanism.

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, if the precondition mechanism is enabled as specified in subclause 5.1.5A; the 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 field; and
- indicate the support for the preconditions mechanism and specify it using the Supported header field.

Upon generating an initial INVITE request using the precondition mechanism, the UE shall not indicate the requirement for the precondition mechanism by using the Require header field.

During the session initiation, if the originating UE indicated the support for the precondition mechanism in the initial INVITE request and:

a) the received response with an SDP body includes a Require header field with "precondition" option-tag, the originating UE shall include a Require header field with the "precondition" option-tag:
   - in subsequent requests that include an SDP body, that the originating UE sends in the same dialog as the response is received from; and
   - in responses with an SDP body to subsequent requests that include an SDP body and include "precondition" option-tag in Supported header field or Require header field received in-dialog; or

b) the received response with an SDP body does not include the "precondition" option-tag in the Require header field,
   - in subsequent requests that include an SDP body, the originating UE shall not include a Require or Supported header field with "precondition" option-tag in the same dialog;

- in responses with an SDP body to subsequent requests with an SDP body but without "precondition" option-tag in the Require or Supported header field, the originating UE shall not include a Require or Supported header field with "precondition" option-tag in the same dialog; and

- in responses with an SDP body to subsequent requests with an SDP body and with "precondition" option-tag in the Require or Supported header field, the originating UE shall include a Require header field with "precondition" option-tag in the same dialog.

NOTE 2: Table A.4 specifies that UE support of forking is required in accordance with RFC 3261 [26]. 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 3: 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 [27]) and does not support the UPDATE request (as described in RFC 3311 [29]).

NOTE 4: The UE can receive a P-Early-Media header field authorizing an early-media flow while the required preconditions, if any, are not met and/or the flow direction is not enabled by the SDP direction parameter. According to RFC 5009 [109], an authorized early-media flow can be established only if the necessary conditions related to the SDP negotiation are met. These conditions can evolve during the session establishment.

NOTE 5: When the UE is confirming the successful resource reservation using an UPDATE request (or a PRACK request) and the UE receives a 180 (Ringing) response or a 200 (OK) response to the initial INVITE request before receiving a 200 (OK) response to the UPDATE request (or a 200 (OK) response to the PRACK request), the UE does not treat this as an error case and does not release the session.

NOTE 6: The UE procedures for rendering of the received early media and of the locally generated communication progress information are specified in 3GPP TS 24.628 [8ZF].

If the UE wishes to receive early media authorization indications, as described in RFC 5009 [109], the UE shall add the P-Early-Media header field with the "supported" parameter to the initial INVITE request.

When a final answer is received for one of the early dialogs, the UE proceeds to set up the SIP session. The UE shall not progress any remaining early dialogs 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.

Upon receiving a 488 (Not Acceptable Here) response to an initial INVITE request, the originating UE should send a new INVITE request containing SDP according to the procedures defined in subclause 6.1.

NOTE 7: An example of where a new request would not be sent is where knowledge exists within the UE, or interaction occurs with the user, such that it is known that the resulting SDP would describe a session that did not meet the user requirements.

Upon receiving a 421 (Extension Required) response to an initial INVITE request in which the precondition mechanism was not used, including the "precondition" option-tag in the Require header field, if the UE supports the precondition mechanism and the precondition mechanism is enabled as specified in subclause 5.1.5A, the originating UE shall:

- send a new INVITE request using the precondition mechanism; and

- send an UPDATE request as soon as the necessary resources are available and a 200 (OK) response for the first PRACK request has been received.

Upon receiving a 503 (Service Unavailable) response to an initial INVITE request containing a Retry-After header field, then the originating UE shall not automatically reattempt the request via the same P-CSCF until after the period indicated by the Retry-After header field contents.

The UE may include a "cic" tel URI parameter in a tel URI, or in the userinfo part of a SIP URI with user=phone, in the Request-URI of an initial INVITE request if the UE wants to identify a user-dialled carrier, as described in RFC 4694 [112].

NOTE 8: The method whereby the UE determines when to include a "cic" tel-URI parameter and what value it should contain is outside the scope of this document (e.g. the UE could use a locally configured digit map to look for special prefix digits that indicate the user has dialled a carrier).

NOTE 9: The value of the "cic" tel-URI parameter reported by the UE is not dependent on UE location (e.g. the reported value is not affected by roaming scenarios).

In the event the UE receives a 380 (Alternative Service) response to an initial INVITE request the response containing a P-Asserted-Identity header field with a value equal to the value of the last entry of 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 7.6.2), the UE shall select a domain in accordance with the conventions and rules specified in 3GPP TS 22.101 [1A] and 3GPP TS 23.167 [4B], and:

- if the CS domain is selected, the UE behaviour is defined in subclause 7.1.2 of 3GPP TS 23.167 [4B] and, where appropriate, in the access technology specific annex; and

- if the IM CN subsystem is selected, the UE shall apply the procedures in subclause 5.1.6 with the exception of selecting a domain for the emergency call attempt.

NOTE 10: The last entry on the Path header field value received during registration is the value of the SIP URI of the P-CSCF. If there are multiple registration flows associated with the registration, then the UE has received from the P-CSCF during registration multiple sets of Path header field values. The last entry of the Path header field value corresponding to the flow on which the 380 (Alternative Service) response was received is checked.

Upon receiving a 199 (Early Dialog Terminated) provisional response to an established early dialog the UE shall release resources specifically related to that early dialog.

The UE shall include the media feature tags as defined in RFC 3840 [62] for all supported streaming media types in the initial INVITE request.

If the UE sends a CANCEL request to cancel an initial INVITE request, the UE shall when applicable include in the CANCEL request a Reason header field with a protocol value set to "RELEASE_CAUSE" and a "cause" header field parameter as specified in subclause 7.2A.18.11.2. The UE may also include the "text" header field parameter with reason-text as specified in subclause 7.2A.18.11.2.

Upon receiving a 500 (Server Internal Error) response to an initial INVITE request including a Reason header field with a protocol value set to "FAILURE_CAUSE" and a cause header field parameter value set to "1" as specified in subclause 7.2A.18.12.2 and a Response-Source header field with a "fe" header field parameter set to "<urn:3gpp:fe:p-cscf.orig>", the UE can determine that the QoS or bearer resources in the originating IP-CAN is not available.

[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 [30] as updated by RFC 4032 [64].

In order to authorize the media streams, the P-CSCF and S-CSCF have to be able to inspect SDP message bodies. Hence, the UE shall not encrypt SDP message bodies.

During the session establishment procedure, and during session modification procedures, SIP messages shall only contain an SDP message body if that is intended to modify the session description, or when the SDP message body is included in the message because of SIP rules described in RFC 3261 [26].

NOTE 1: A codec can have multiple payload type numbers associated with it.

In order to support accurate bandwidth calculations, the UE may include the "a=ptime" attribute for all "audio" media lines as described in RFC 4566 [39]. If a UE receives an "audio" media line with "a=ptime" specified, the UE should transmit at the specified packetization rate. If a UE receives an "audio" media line which does not have "a=ptime" specified or the UE does not support the "a=ptime" attribute, the UE should transmit at the default codec packetization rate as defined in RFC 3551 [55A]. The UE will transmit consistent with the resources available from the network.

For "video" and "audio" media types that use the RTP/RTCP and where the port number is not zero, the UE shall specify the proposed bandwidth for each media stream using the "b=" media descriptor and the "AS" bandwidth modifier in the SDP.

NOTE 2: The above is the minimum requirement for all UEs. Additional requirements can be found in other specifications.

For "video" and "audio" media types that use the RTP/RTCP and where the port number is not zero, the UE may include for each RTP payload type "a=bw-info" SDP attribute(s) (defined in clause 19 of 3GPP TS 26.114 [9B]) to indicate the additional bandwidth information. The "a=bw-info" SDP attribute line(s) shall be specified in accordance with 3GPP TS 26.114 [9B]. The value of the "a=bw-info" SDP attribute(s) may affect the assigned QoS which is defined in 3GPP TS 29.213 [13C].

For "video" and "audio" media types that utilize the RTP/RTCP, in addition to the "b=AS" parameter, the UE may specify the "b=TIAS", and "a=maxprate" parameters in accordance with RFC 3890 [152]. The value of the parameter shall be determined as described in RFC 3890 [152]. The value or absence of the "b=" parameter(s) may affect the assigned QoS which is defined in 3GPP TS 29.213 [13C].

If a UE receives a media line which contains both a=ptime and a=maxprate, the UE should use the a=maxprate value, if this attribute is supported.

If multiple codecs are specified on the media line, "a=maxprate" (or "a=ptime" if "a=maxprate" is not available or not supported) should be used to derive the packetization time used for all codecs specified on the media line. Given that not all codecs support identical ranges of packetization, the UE should ensure that the packetization derived by "a=maxprate" (or "a=ptime" if "a=maxprate" is not available or not supported) is a valid packetization time for each codec specified in the list.

If the media line in the SDP message body 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 [56], 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 [56] 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 [152].

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 [13C].

NOTE 3: 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.

If an in-band DTMF codec is supported by the application associated with an audio media stream, then the UE shall include, in addition to the payload type numbers associated with the audio codecs for the media stream, for each clock rate associated with the audio codecs for the media stream, a payload type number associated with the MIME subtype "telephone-event", to indicate support of in-band DTMF as described in RFC 4733 [23].

The UE shall inspect the SDP message body contained in any SIP request or response, looking for possible indications of grouping of media streams according to RFC 3524 [54] 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, subclause L.2.2.5 for IP-CAN implemented using EPS, and subclause U.2.2.5 for IP-CAN implemented using 5GS).

In case of UE initiated resource reservation and if the UE determines 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 4: 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 UE shall indicate as met the local preconditions related to the media stream, for which resources are re-used.

If the SDP is affected due to a rejected IP-CAN bearer or a released IP-CAN bearer then the UE shall:

1) update the session according to RFC 3264 [27B] and set the ports of the media stream(s) for which IP-CAN resource was rejected or released to zero in the new SDP offer;

2) release the session according to RFC 3261 [26];

3) cancel the session setup or the session modification according to RFC 3261 [26]; or

4) reject the session setup or the session modification according to RFC 3261 [26].

If the SDP is affected due to a modified IP-CAN bearer, and the desired QoS resources for one or more media streams are no longer available at the UE due to the modification, then the UE shall:

1) update the session according to RFC 3264 [27B] and set the ports of the media stream(s) for which IP-CAN resource was modified to zero in the new SDP offer;

2) release the session according to RFC 3261 [26];

3) cancel the session setup or the session modification according to RFC 3261 [26]; or

4) reject the session setup or the session modification according to RFC 3261 [26].

NOTE 5: The UE can use one IP address for signalling (and specify it in the Contact header field) and different IP address(es) for media (and specify it in the "c=" parameter of the SDP).

If the UE wants to transport media streams with TCP and there are no specific alternative negotiation mechanisms defined for that particular application, then the UE shall support the procedures and the SDP rules specified in RFC 4145 [83].

The UE may support being configured with a media type restriction policy using one or more of the following methods:

a) the Media_type_restriction_policy node of the $EF_{IMSConfigData}$ file described in 3GPP TS 31.102 [15C];

b) the Media_type_restriction_policy node of the $EF_{IMSConfigData}$ file described in 3GPP TS 31.103 [15B]; and

c) the Media_type_restriction_policy node of 3GPP TS 24.167 [8G].

If the UE is configured with both the Media_type_restriction_policy node of 3GPP TS 24.167 [8G] and the Media_type_restriction_policy node of the $EF_{IMSConfigData}$ file described in 3GPP TS 31.102 [15C] or 3GPP TS 31.103 [15B, then the Media_type_restriction_policy node of the $EF_{IMSConfigData}$ file shall take precedence.

NOTE 6: Precedence for files configured on both the USIM and ISIM is defined in 3GPP TS 31.103 [15B].

If the UE supports being configured with a media type restriction policy, the UE shall not include in a sent SDP message (SDP offer or SDP answer) a media stream with:

- non zero port number; and

- a media type which is restricted from inclusion in an SDP message according to the media type restriction policy.

NOTE 7: 488 (Not Acceptable Here) response is sent when all media types of all media streams of an SDP offer are restricted from inclusion in an SDP message according to the media type restriction policy.
[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. This 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 [30] and RFC 4032 [64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value either "optional" or as specified in RFC 3312 [30] and RFC 4032 [64] for the remote segment, if the UE uses the precondition mechanism (see subclause 5.1.3.1); and

- if the UE uses the precondition mechanism (see subclause 5.1.3.1), shall not request confirmation for the result of the resource reservation (as defined in RFC 3312 [30]) at the terminating UE.

NOTE 1: Previous versions of this document mandated the use of the SDP inactive attribute. This document does not prohibit specific services from using direction attributes to implement their service-specific behaviours.

If the UE uses the precondition mechanism (see subclause 5.1.3.1), and 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 [30] and RFC 4032 [64], as well as the strength-tag value "mandatory" for the local segment and the strength-tag value either "optional" or as specified in RFC 3312 [30] and RFC 4032 [64] for the remote segment and shall not request confirmation for the result of the resource reservation (as defined in RFC 3312 [30]) at the terminating UE.

NOTE 2: If the originating UE does not use the precondition mechanism (see subclause 5.1.3.1), it will not include any precondition information in the SDP message body.

If the UE indicated support for end-to-access-edge media security using SDES during registration, and the P-CSCF indicated support for end-to-access-edge media security using SDES during registration, then upon generating an SDP offer with an RTP based media, for each RTP based media except those for which the UE requests an end-to-end media security mechanism, the UE shall:

- offer SRTP transport protocol according to RFC 3711 [169] and the profile defined in 3GPP TS 33.328 [19C];

- include the SDP crypto attribute according to RFC 4568 [168] and the profile defined in 3GPP TS 33.328 [19C]; and

- include an SDP "a=3ge2ae:requested" attribute.

If the UE indicated support for the end-to-access-edge media security for MSRP using TLS and certificate fingerprints during registration, and the P-CSCF indicated support for the end-to-access-edge media security for MSRP using TLS and certificate fingerprints during registration, then upon generating an SDP offer with an MSRP based media, for each MSRP based media except those for which the UE requests an end-to-end security mechanism, the UE shall:

- offer MSRP over TLS transport protocol according to RFC 4975 [178], RFC 6714 [214] and the profile defined in 3GPP TS 33.328 [19C];

- include the SDP fingerprint attribute according to RFC 8122 [241] and the profile defined in 3GPP TS 33.328 [19C]; and

- include the SDP "a=3ge2ae:requested" attribute.

NOTE 3: TLS client role and TLS server role are determined according to RFC 6135 [215] (referenced by RFC 6714 [214]). If the SDP answer contains the SDP setup attribute with "active" attribute value, the answerer performs the TLS client role. If the SDP answer contains the SDP setup attribute with "passive" attribute value, the offerer performs the TLS client role.

If the UE indicated support for the end-to-access-edge media security for BFCP using TLS and certificate fingerprints during registration, and the P-CSCF indicated support for the end-to-access-edge media security for BFCP using TLS and certificate fingerprints during registration, then upon generating an SDP offer with an BFCP based media, for each BFCP based media except those for which the UE requests an end-to-end security mechanism, the UE shall:

- offer BFCP over TLS transport protocol according to RFC 4583 [108] and the profile defined in 3GPP TS 33.328 [19C];

- include the SDP fingerprint attribute according to RFC 8122 [241] and the profile defined in 3GPP TS 33.328 [19C]; and

- include the SDP "a=3ge2ae:requested" attribute.

Unless a new TLS session is negotiated, subsequent SDP offers and answers shall not impact the previously negotiated TLS roles.

NOTE 4: RFC 4583 [108] specifies that the SDP answerer will act as the TLS server but leaves the impact of SDP renegotiation on TLS unspecified.

If the UE indicated support for the end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints during registration, and the P-CSCF indicated support for the end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints during registration, then upon generating an SDP offer with an UDPTL based media, for each UDPTL based media except those for which the UE requests an end-to-end security mechanism, the UE shall:

- offer UDPTL over DTLS transport protocol according to RFC 7345 [217], draft-ietf-mmusic-dtls-sdp [240] and the profile defined in 3GPP TS 33.328 [19C];
- include the SDP fingerprint attribute according to RFC 8122 [241] and the profile defined in 3GPP TS 33.328 [19C];
- include the SDP "a=3ge2ae:requested" attribute; and
- include the SDP tls-id attribute according to draft-ietf-mmusic-dtls-sdp [240].

If the P-CSCF did not indicate support for end-to-access-edge media security using SDES during registration, the UE shall not include an SDP "a=3ge2ae:requested" attribute in any RTP based media in any SDP offer.

If the P-CSCF did not indicate support for the end-to-access-edge media security for MSRP using TLS and certificate fingerprints during registration, the UE shall not include an SDP "a=3ge2ae:requested" attribute in any MSRP based media in any SDP offer.

If the P-CSCF did not indicate support for the end-to-access-edge media security for BFCP using TLS and certificate fingerprints during registration, the UE shall not include an SDP "a=3ge2ae:requested" attribute in any BFCP based media in any SDP offer.

If the P-CSCF did not indicate support for the end-to-access-edge media security for UDPTL using DTLS and certificate fingerprints during registration, the UE shall not include an SDP "a=3ge2ae:requested" attribute in any UDPTL based media in any SDP offer.

The UE shall not include an SDP "a=3ge2ae:requested" attribute in any media other than RTP based, MSRP based, BFCP based and UDPTL based in any SDP offer.

Upon generating an SDP offer with an MSRP based media protected by the end-to-end media security for MSRP using TLS and KMS, the UE shall:

- offer MSRP over TLS transport protocol according to RFC 4975 [178], RFC 6714 [214] and the profile defined in 3GPP TS 33.328 [19C]; and
- include the SDP key-mgmt attribute according to RFC 4567 [167] and the profile defined in 3GPP TS 33.328 [19C];

NOTE 5: SDP fingerprint attribute is not included.

Upon receiving an SDP answer to the SDP offer with the MSRP based media protected by the end-to-end media security for MSRP using TLS and KMS, and if the MSRP based media is accepted and associated with the SDP key-mgmt attribute as described in RFC 4567 [167] and the profile defined in 3GPP TS 33.328 [19C] in the SDP answer, then the UE indicate the pre-shared key ciphersuites according to RFC 4279 [218] and the profile defined in 3GPP TS 33.328 [19C] in TLS handshake of TLS connection transporting the MSRP based media.

When the UE detects that an emergency call is being made, the UE shall not include end-to-end media security on any media in the SDP offer.

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 SDP offer shall contain a subset of the allowed media types, codecs and other parameters from the SDP message bodies of all 488 (Not Acceptable Here) responses so far received for the same session establishment attempt (i.e. a set of INVITE requests used for the same session establishment). For each media line, the UE shall order the codecs in the SDP offer according to the order of the codecs in the SDP message bodies of the 488 (Not Acceptable Here) responses.

NOTE 6: 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 message bodies 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 an SDP offer in which the related local preconditions are set to met, using the segmented status type, as defined in RFC 3312 [30] and RFC 4032 [64].

Upon receiving an SDP answer, which includes more than one codec per media stream, excluding the in-band DTMF codec, as described in subclause 6.1.1, the UE shall:

- send an SDP offer at the first possible time, selecting only one codec per media stream; or

- if the UE is participant in a multi-stream multiparty multimedia conference session using simulcast (indicated by the presence of "a=simulcast" SDP attribute(s) in the SDP answer, as defined in draft-ietf-mmusic-sdp-simulcast [249]), apply the procedures defined in 3GPP TS 26.114 [9B] annex S.

If the UE sends an initial INVITE request that includes only an IPv6 address in the SDP offer, and receives an error response (e.g., 488 (Not Acceptable Here) with 301 Warning header field) indicating "incompatible network address format", the UE shall send an ACK as per standard SIP procedures. Subsequently, the UE may acquire an IPv4 address or use an existing IPv4 address, and send a new initial INVITE request to the same destination containing only the IPv4 address in the SDP offer.

[TS 26.114, clause 5.2.1.1]:

MTSI clients in terminals offering speech communication shall support narrowband, wideband and super-wideband communication.

In addition, MTSI clients in terminals offering speech communication shall support:

- AMR speech codec (3GPP TS 26.071 [11], 3GPP TS 26.090 [12], 3GPP TS 26.073 [13] and 3GPP TS 26.104 [14]) including all 8 modes and source controlled rate operation 3GPP TS 26.093 [15]. The MTSI client in terminal shall be capable of operating with any subset of these 8 codec modes. More detailed codec requirements for the AMR codec are defined in clause 5.2.1.2.

MTSI clients in terminals offering wideband speech communication at 16 kHz sampling frequency shall support:

- AMR-WB codec (3GPP TS 26.171 [17], 3GPP TS 26.190 [18], 3GPP TS 26.173 [19] and 3GPP TS 26.204 [20]) including all 9 modes and source controlled rate operation 3GPP TS 26.193 [21]. The MTSI client in terminal shall be capable of operating with any subset of these 9 codec modes. More detailed codec requirements for the AMR-WB codec are defined in clause 5.2.1.3. When the EVS codec is supported, the EVS AMR-WB IO mode may serve as an alternative implementation of AMR-WB as defined in clause 5.2.1.4.

MTSI clients in terminals offering super-wideband or fullband speech communication shall support:

- EVS codec (TS 26.441 [121], TS 26.444 [124], TS 26.445 [125], TS 26.447 [127], TS 26.451 [131], TS 26.442 [122] and TS 26.443 [123]) as described below including functions for backwards compatibility with AMR-WB (TS 26.446 [126]) and discontinuous transmission (TS 26.449 [129] and TS 26.450 [130]). More detailed codec requirements for the EVS codec are defined in clause 5.2.1.4.

Encoding of DTMF is described in Annex G.

[TS 26.114, clause 6.2.2.1]:

For AMR or AMR-WB encoded media, the session setup shall determine the applicable bandwidth(s) as defined in clause 6.2.5, what RTP profile to use; if all codec modes can be used or if the operation needs to be restricted to a subset; if the bandwidth-efficient payload format can be used or if the octet-aligned payload format must be used; if codec mode changes shall be restricted to be aligned to only every other frame border or if codec mode changes can occur at any frame border; if codec mode changes must be restricted to only neighbouring modes within the negotiated codec mode set or if codec mode changes can be performed to any mode within the codec mode set; the number of speech frames that should be encapsulated in each RTP packet and the maximum number of speech frames that may be encapsulated in each RTP packet. For EVS encoded media, the session setup shall determine the RTP profile to use in the session.

If the session setup negotiation concludes that multiple configuration variants are possible in the session then the default operation should be used as far as the agreed parameters allow, see clause 7.5.2.1. It should be noted that the default configurations are slightly different for different access types.

An MTSI client offering a speech media session for narrow-band speech and/or wide-band speech should generate an SDP offer according to the examples in Annexes A.1 to A.3. An MTSI client offering EVS should generate an SDP offer according to the examples in Annex A.14.

An MTSI client in terminal supporting EVS should support the RTCP-APP signalling for speech adaptation defined clause 10.2.1, and shall support the RTCP-APP signalling when the MTSI client in terminal supports adaptation for call cases where the RTP-based CMR cannot be used.

NOTE: Examples of call cases where the RTP-based CMR cannot be used are: when the RTP-based CMR is disabled; or for uni-directional media (sendonly or recvonly).

Some of the request messages are generic for all speech codecs while other request messages are codec-specific. Request messages that can be used in a session are negotiated in SDP, see clause 10.2.3.

An MTSI client shall at least offer AVP for speech media streams. An MTSI client should also offer AVPF for speech media streams. An MTSI client shall offer AVPF for speech media streams when offering to use RTCP-APP signalling. RTP profile negotiation shall be done as described in clause 6.2.1a. When AVPF is offered then the RTCP bandwidth shall be greater than zero.

If an MTSI client in terminal offers to use ECN for speech in RTP streams then the MTSI client in terminal shall offer ECN Capable Transport as defined below. If an MTSI client in terminal accepts an offer for ECN for speech then the MTSI client in terminal shall declare ECN Capable Transport in the SDP answer as defined below. The SDP negotiation of ECN Capable Transport is described in [84].

ECN shall not be used when the codec negotiation concludes that only fixed-rate operation is used.

An MTSI client may support multiple codecs where ECN-triggered adaptation is supported only for some of the codecs. An SDP offer for ECN may therefore include multiple codecs where ECN-triggered adaptation is supported only for some of the codecs. An MTSI client receiving an SDP offer including multiple codecs and an offer for ECN should first select which codec to accept and then accept or reject the offer for ECN depending on whether ECN-triggered adaptation is supported for that codec or not. An MTSI client receiving an SDP answer accepting ECN for a codec where ECN-triggered adaptation is not supported should re-negotiate the session to disable ECN.

NOTE: ECN-triggered adaptation is currently undefined for EVS. This does not prevent ECN-triggered adaptation from being negotiated and used for AMR or AMR-WB.

The use of ECN for a speech stream in RTP is negotiated with the 'ecn-capable-rtp' SDP attribute, [84]. ECN is enabled when both clients agree to use ECN as configured below. An MTSI client in terminal using ECN shall therefore also include the following parameters and parameter values for the ECN attribute:

- 'leap', to indicate that the leap-of-faith initiation method shall be used;
- 'ect=0', to indicate that ECT(0) shall be set for every packet.

An MTSI client offering ECN for speech may indicate support of the RTCP AVPF ECN feedback messages [84] using "rtcp-fb" attributes with the "nack" feedback parameter and the "ecn" feedback parameter value. An MTSI client offering ECN for speech may indicate support for RTCP XR ECN summary reports [84] using the "rtcp-xr" SDP attribute [88] and the "ecn-sum" parameter.

An MTSI client receiving an offer for ECN for speech without an indication of support of RTCP AVPF ECN feedback messages [84] within an "rtcp-fb" attribute should accept the offer if it supports ECN.

An MTSI client receiving an offer for ECN for speech with an indication of support of the RTCP AVPF ECN feedback message [84] should also accept the offer and may indicate support of the RTCP AVPF ECN feedback messages [84] in the answer.

An MTSI client accepting ECN for speech in an answer may indicate support for RTCP XR ECN summary reports in the answer using the "rtcp-xr" SDP attribute [88] and the "ecn-sum" parameter.

The use of ECN is disabled when a client sends an SDP without the 'ecn-capable-rtp' SDP attribute.

An MTSI client may initiate a session re-negotiation to disable ECN to resolve ECN-related error cases. An ECN-related error case may, for example, be detecting non-ECT in the received packets when ECT(0) was expected or detecting a very high packet loss rate when ECN is used.

SDP examples for offering and accepting ECT are shown in Annex A.12.

Session setup for sessions including speech and DTMF events is described in Annex G.

[TS 26.114, clause 6.2.5.1]:

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 [8].

An MTSI client in terminal should include the 'a=bw-info' attribute in the SDP offer. When accepting a media type where the 'a=bw-info' attribute is included the MTSI client in terminal shall include the 'a=bw-info' attribute in the SDP answer if it supports the attribute. The 'a=bw-info' attribute and the below used bandwidth properties are defined in clause 19.

When the 'a=bw-info' attribute is supported, the following bandwidth properties shall be included for each RTP payload type in the SDP:

- Maximum Supported Bandwidth for sending direction.
- Maximum Desired Bandwidth for sending direction.
- Minimum Desired Bandwidth for sending direction.
- Minimum Supported Bandwidth for sending direction.
- Maximum Supported Bandwidth for receiving direction with the following exception:
  - The b=AS bandwidth modifier indicates the bandwidth needed for the RTP payload type that requires the highest bandwidth. The Maximum Supported Bandwidth for this RTP payload type is therefore indicated with the b=AS bandwidth modifier and does not need to be indicated with the 'a=bw-info' attribute for this RTP payload type. It is still allowed to include the 'a=bw-info' attribute for this RTP payload type but the value shall then be aligned with the b=AS value when sending the SDP. When receiving the SDP, the b=AS bandwidth modifier and the Maximum Supported Bandwidth for the receiving direction may not be aligned. In this case, the maximum sending rate is determined as defined below.
- Maximum Desired Bandwidth for receiving direction.
- Minimum Desired Bandwidth for receiving direction.
- Minimum Supported Bandwidth for receiving direction.

Recommended bandwidths for several codec configurations are provided in the media-specific sections.

For a media stream that has been removed by either the offerer or answerer, the inclusion of bandwidth information is optional. This is in accordance with clause 8.2 of RFC 3264 [58].

SDP examples incorporating bandwidth modifiers are shown in annex A. SDP examples using the 'a=bw-info' attribute are shown in annex A.6.3.

When an MTSI client in terminal receives an SDP offer or answer it shall determine the maximum sending rate for the selected codec by selecting the smallest of the following:

- the bandwidth value, if the b=AS parameter was included in the received SDP offer or answer
- the Maximum Supported Bandwidth for the receiving direction, if included in the received SDP
- the preconfigured data rate for the selected codec, if the MTSI client has been preconfigured by the operator to use a particular data rate for the selected codec
- the maximum data rate for the selected codec as determined by examining the codec information (e.g., codec, mode, profile, level) and any other media information (e.g., ptime and maxptime) included in the received SDP offer or answer. This maximum data rate is determined assuming no extra bandwidth is allowed for redundancy.

The maximum sending rate may be further updated by the MTSI client in terminal based on receiving an indication of the granted QoS (see clause 6.2.7).

The MTSI client in terminal shall not transmit at a rate above the maximum sending rate. For speech, the MTSI client should transmit using the codec mode with the highest data rate allowed by the maximum sending rate, except if limited to a lower codec mode by the initial codec mode procedures (see clause 7.5.2.1.6) or by the adaptation procedures (see clause 10.2).

The MTSI client in terminal may support access network bitrate recommendation (ANBR, see clause 10.7). SDP offer/answer re-negotiation shall not be used as a replacement for dynamic media bitrate adaptation. ANBR contains information on short-term bandwidth and SDP offer/answer re-negotiations should be avoided or minimized since they consume network resources. Therefore, SDP offer/answer re-negotiation (e.g. in SIP UPDATE) shall not be initiated based on ANBR information other than in the following cases:

If;

1. The received ANBR from the access network is below the established GBR; and
2. The received ANBR cannot be supported by any of the negotiated codec configurations; and
3. Potentially increased loss and/or delay due to not lowering the bitrate are not acceptable; and
4. The MTSI client in terminal supports one or more codec configurations that supports the received ANBR; and
5. ANBR messages with values meeting all conditions in 1-4 above are received consistently for an extensive period of time (e.g. 5 seconds or more, see also clause 10.7.2)

then the MTSI client in terminal:

- may re-negotiate the session
  - To switch to a codec or codec configuration that can support the lower bitrate in the ANBR (if any); and/or
  - To reduce the number of used RTP streams (e.g. turning off the affected media); and
- If the session re-negotiation fails, shall not initiate further re-negotiation based on ANBR for that bearer in the session.

For video, if:

- TMMBR/TMMBN are not supported in the session; and
- For an extensive period of time (e.g. 5 seconds), the MTSI client in terminal consistently receives ANBR messages with values significantly below the video bitrate sent (as estimated by the receiving MTSI client in terminal) from the remote peer

Then the MTSI client in terminal may re-negotiate the session:

- To set the session bitrate for video (see clause 6.2.5) to a value corresponding to the minimum of the received ANBR and GBR (if > 0); or
- To turn video off

NOTE 1: An ANBR below GBR does not change the GBR semantics in any way. GBR is defined as a guarantee that for a packet stream not exceeding the GBR, 98 percent of the packets do not experience a delay exceeding the QCI's Packet Delay Budget (see clause 6.1.7.2 of 3GPP TS 23.303 [90]). Temporarily reducing bitrate below GBR to comply with an ANBR can increase the probability that loss and/or delay can be kept within the bounds set by the used QCI.

NOTE 2: For GBR=MBR bearers, an ANBR below the GBR can frequently be supported by the negotiated codec configuration.

NOTE 3: For GBR<MBR bearers, an ANBR below the GBR can typically not be supported by the negotiated codec configuration.

NOTE 4: If the above conditions are not met, the MTSI client in terminal will ignore ANBR values below the GBR (see also clause 10.7.2).
[TS 26.114, clause 7.3.1]:

The RTP implementation shall include an RTCP implementation.

For a given RTP based media stream, the MTSI client in terminal shall use the same port number for sending and receiving RTCP packets. This facilitates interworking with fixed/broadband access. However, the MTSI client shall accept RTCP packets that are not received from the same remote port where RTCP packets are sent by the MTSI client.

The bandwidth for RTCP traffic shall be described using the "RS" and "RR" SDP bandwidth modifiers at media level, as specified by RFC 3556 [42]. Therefore, an MTSI client 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:

- 8 000 bps for the RS field (at media level);
- 6 000 bps for the RR field (at media level).

The RS and RR values included in the SDP answer should be treated as the negotiated values for the session and should be used to calculate the total RTCP bandwidth for all terminals in the session.

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.

If a MTSI client receives SDP bandwidth modifiers for RTCP equal to zero from the originating MTSI client, it should reply (via the SIP protocol) by setting its RTCP bandwidth using SDP bandwidth modifiers with values equal to zero.

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. The RR value should be set greater than zero to enable RTCP packets to be sent when media is put on hold and during active RTP media transmission, including real-time text sessions which may have infrequent RTP media transmissions.

Point-to-point speech only sessions may not require the above 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 the SDP bandwidth modifier RR value set greater than zero, and send RTCP packets (i.e., Receiver Reports) to the other end. This allows the remote end to detect link aliveness during hold. When media is resumed, the resuming MTSI client should request to turn off the RTCP sending again through a re-negotiation of the RTCP bandwidth with SDP bandwidth modifiers equal to zero.

When RTCP is turned off (for point-to-point speech only sessions) and if sending of an additional associated RTP stream becomes required and both RTP streams need to be synchronized, or if transport feedback due to lack of end-to-end QoS guarantees is needed, a MTSI client should re-negotiate the bandwidth for RTCP by sending an SDP with the RR bandwidth modifier greater than zero. Setting the RR bandwidth modifier greater than zero allows sending of RTCP Receiver Reports even when the session is put on hold and neither terminal is actively sending RTP media.

NOTE 1: Deactivating RTCP will disable the adaptation mechanism for speech defined in clause 10.2.

7.4.3 Test description

7.4.3.1 Pre-test conditions

System Simulator:

- 1 NR Cell connected to 5GC, default parameters.

UE:

- The UE contains either ISIM and USIM applications or only USIM application on UICC.
- The UE is configured to register for IMS after switch on.

Preamble:

- UE is in state 1N-A and registered to IMS

7.4.3.2 Test procedure sequence

Table 7.4.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	UE is made to attempt an IMS voice call.				
2	Step 1 of Annex A.4.1 happens	-->	INVITE	1	P
3	Step 2 of Annex A.4.1 happens	<--	100 Trying		
4	Step 3 of Annex A.4.1 happens	<--	183 Session Progress		
5	Step 4 of Annex A.4.1 happens	-->	PRACK	2	P
6	Step 5 of Annex A.4.1 happens	<--	200 OK		
7	Step 6 of Annex A.4.1 happens	-->	UPDATE	3	P
8	Step 7 of Annex A.4.1 happens	<--	200 OK		
9	Step 8 of Annex A.4.1 happens	<--	180 Ringing		
10	Step 9 of Annex A.4.1 happens	-->	PRACK	4	P
11	Step 10 of Annex A.4.1 happens	<--	200 OK		
12	Step 11 of Annex A.4.1 happens	<--	200 OK		
13	Step 12 of Annex A.4.1 happens	-->	ACK	5	P
NOTE: The test procedure including NR/5GC signalling is specified in TS 38.508 [21] subclause 4.9.15.					

7.4.3.3 Specific message contents

None as fully described in Annex A.4.1.

7.5 MTSI MO Voice Call without preconditions at both originating UE and terminating UE / 5GS

7.5.1 Test Purpose (TP)

(1)

```
with { UE being registered to IMS and configured to not use preconditions }
ensure that {
  when { UE is being made to initiate a voice call }
    then { UE sends INVITE for voice call without preconditions }
            }
```

(2)

```
with { UE having sent INVITE without preconditions }
ensure that {
  when { UE receives 183 Session Progress without preconditions }
    then { UE sends PRACK for 183 Session Progress }
            }
```

(3)

```
with { UE having sent PRACK }
ensure that {
  when { UE receives 200 OK for PRACK followed by 180 Ringing followed by 200 OK for INVITE }
    then { UE sends ACK }
            }
```

7.5.2 Conformance Requirements

As described in 7.4.2 except:

[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 [30] as updated by RFC 4032 [64].

The preconditions mechanism should be supported by the originating UE.

If the precondition mechanism is disabled as specified in subclause 5.1.5A, the UE shall not use the precondition mechanism.

[TS 24.229, clause 5.1.5A]:

The precondition disabling policy indicates whether the UE is allowed to use the precondition mechanism or whether the UE is not allowed to use the precondition mechanism.

If the precondition disabling policy is not configured, the precondition disabling policy is assumed to indicate that the UE is allowed to use the precondition mechanism.

The UE may support the precondition disabling policy.

If the UE supports the precondition disabling policy, the UE may support being configured with the precondition disabling policy using one or more of the following methods:

a) the Precondition_disabling_policy node of the $EF_{IMSConfigDat}$a file described in 3GPP TS 31.102 [15C];

b) the Precondition_disabling_policy node of the $EF_{IMSConfigData}$ file described in 3GPP TS 31.103 [15B]; and

c) the Precondition_disabling_policy node of 3GPP TS 24.167 [8G].

If the UE is configured with both the Precondition_disabling_policy node of 3GPP TS 24.167 [8G] and the Precondition_disabling_policy node of the $EF_{IMSConfigData}$ file described in 3GPP TS 31.102 [15C] or 3GPP TS 31.103 [15B], then the Precondition_disabling_policy node of the $EF_{IMSConfigData}$ file shall take precedence.

NOTE: Precedence for files configured on both the USIM and ISIM is defined in 3GPP TS 31.103 [15B].

The precondition mechanism is disabled, if the UE supports the precondition disabling policy and the precondition disabling policy indicates that the UE is not allowed to use the precondition mechanism.

The precondition mechanism is enabled, if:

1) the UE does not support the precondition disabling policy; or

2) the UE supports the precondition disabling policy and the precondition disabling policy indicates that the UE is allowed to use the precondition 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. This SDP offer shall reflect the calling user's terminal capabilities and user preferences for the session.

…

NOTE 2: If the originating UE does not use the precondition mechanism (see subclause 5.1.3.1), it will not include any precondition information in the SDP message body.

Reference(s)

3GPP TS 24.229 [7], clauses 5.1.3.1, 5.1.5A and 6.1.2.

7.5.3 Test description

7.5.3.1 Pre-test conditions

System Simulator:

- 1 NR Cell connected to 5GC, default parameters.

UE:

- UE contains either ISIM and USIM applications or only USIM application on UICC.
- UE is configured to register for IMS after switch on.
- UE is configured to not use the precondition mechanism.

Preamble:

- The UE is in test state 1N-A (TS 38.508-1) and registered to IMS.

7.5.3.2 Test procedure sequence

Table 7.5.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	UE is made to attempt an IMS voice call.				
2	Step 1 of Annex A.4.2 happens	-->	INVITE	1	P
3	Step 2 of Annex A.4.2 happens	<--	100 Trying		
4	Step 3 of Annex A.4.2 happens	<--	183 Session Progress		
5	Step 4 of Annex A.4.2 happens	-->	PRACK	2	P
6	Step 5 of Annex A.4.2 happens	<--	200 OK		
7	Step 6 of Annex A.4.2 happens	<--	180 Ringing		
8	Step 7 of Annex A.4.2 happens	<--	200 OK		
9	Step 8 of Annex A.4.2 happens	-->	ACK	3	P
NOTE: The test procedure including NR/5GC signalling is specified in TS 38.508 [21] subclause 4.9.15.					

7.5.3.3 Specific message contents

None as fully described in annex A.4.2.

7.6 MTSI MT Voice Call with preconditions at both originating UE and terminating UE / 5GS

7.6.1 Test Purpose (TP)

(1)

```
with { UE being registered to IMS }
ensure that {
  when { UE receives INVITE for voice call }
    then { UE responds with 183 Session Progress including SDP }
            }
```

(2)

```
with { UE having sent 183 Session Progress }
ensure that {
  when { UE receives PRACK for 183 Session Progress }
    then { UE sends 200 OK for PRACK }
            }
```

(3)

```
with { UE having sent 200 OK for PRACK }
ensure that {
  when { UE receives UPDATE including SDP }
    then { UE sends 200 OK for UPDATE including SDP and 180 Ringing }
            }
```

(4)

```
with { UE having sent 180 Ringing, possibly reliably }
ensure that {
  when { 180 was sent reliably and consequently UE receives PRACK for 180 Ringing }
    then { UE sends 200 OK for PRACK }
            }
```

(5)

```
with { UE having sent 180 Ringing  }
ensure that {
  when { User accepts the incoming voice call request }
    then { UE sends 200 OK for INVITE }
            }
```

(6)

```
with { UE having sent 200 OK for INVITE }
ensure that {
  when { UE receives ACK followed by BYE }
    then { UE sends 200 OK for BYE }
            }
```

7.6.2 Conformance Requirements

Editor's note: more concrete texts for supporting the TPs need to be investigated.

[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.

During the session initiation, 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 field or Require header field and the precondition mechanism is enabled as specified in subclause 5.1.5A, the terminating UE shall use the precondition mechanism and shall include a Require header field with the "precondition" option-tag:

…

If the terminating UE included an SDP offer or an SDP answer in a reliable provisional response to the INVITE request and both the terminating UE and the originating UE support UPDATE method, then in order to remove one or more media streams negotiated in the session for which a final response to the INVITE request has not been sent yet, the terminating UE shall send an UPDATE request with a new SDP offer and delays sending of 200 (OK) response to the INVITE request till after reception of 200 (OK) response to the UPDATE request.

If the user does not accept a media stream accepted in the SDP answer and the terminating UE, the originating UE or both do not support the UPDATE method, then after reception of ACK request related to 200 (OK) response to the INVITE request, the UE shall modify the session.

The terminating UE shall include the media feature tags as defined in RFC 3840 [62] for all supported streaming media types in the SIP response other than the 100 (Trying) response to the SIP INVITE request.

[TS 24.229, clause 6.1.1]

During the session establishment procedure, and during session modification procedures, SIP messages shall only contain an SDP message body if that is intended to modify the session description, or when the SDP message body is included in the message because of SIP rules described in RFC 3261 [26].

[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, the UE shall set the media streams to active mode by applying the procedures described in RFC 4566 [39] with respect to setting the direction of media streams.

…

Upon sending an 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 used by the terminating UE (see subclause 5.1.4.1), 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]

In addition, MTSI clients in terminals offering speech communication shall support:

- AMR speech codec (3GPP TS 26.071 [11], 3GPP TS 26.090 [12], 3GPP TS 26.073 [13] and 3GPP TS 26.104 [14]) including all 8 modes and source controlled rate operation 3GPP TS 26.093 [15]. The MTSI client in terminal shall be capable of operating with any subset of these 8 codec modes. More detailed codec requirements for the AMR codec are defined in clause 5.2.1.2.

[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 generate an SDP offer according to the examples in Annexes A.1 to A.3. An MTSI client offering EVS should generate an SDP offer according to the examples in Annex A.14.

An MTSI client in terminal supporting EVS should support the RTCP-APP signalling for speech adaptation defined clause 10.2.1, and shall support the RTCP-APP signalling when the MTSI client in terminal supports adaptation for call cases where the RTP-based CMR cannot be used.

[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 [8].

[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 [42].

Reference(s)

3GPP TS 24.229 clauses 5.1.4.1, 6.1.1, 6.1.3, TS 26.114 clause 5.2.1, 6.2.2.1, 6.2.5 and 7.3.1.

7.6.3 Test description

7.6.3.1 Pre-test conditions

System Simulator:

- 1 NR Cell connected to 5GC, default parameters.

UE:

- UE contains either ISIM and USIM applications or only USIM application on UICC.
- UE is configured to register for IMS after switch on.
- UE is configured to use the precondition mechanism.

Preamble:

- The UE is in test state 1N-A (TS 38.508-1) and registered to IMS.

7.6.3.2 Test procedure sequence

Table 7.6.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	Step 1 of Annex A.5.1 happens	<--	INVITE		
2	Step 2 of Annex A.5.1 happens	-->	100 Trying		
3	Step 3 of Annex A.5.1 happens	-->	183 Session Progress	1	P
4	Step 4 of Annex A.5.1 happens	<--	PRACK		
5	Step 5 of Annex A.5.1 happens	-->	200 OK	2	P
6	Step 6 of Annex A.5.1 happens	<--	UPDATE		
7	Step 7 of Annex A.5.1 happens	-->	200 OK	3	P
8	Step 8 of Annex A.5.1 happens	-->	180 Ringing		
9	Step 9 of Annex A.5.1 happens	<--	PRACK		
10	Step 10 of Annex A.5.1 happens	-->	200 OK	4	P
11	Step 11 of Annex A.5.1 happens	-->	200 OK	5	P
12	Step 12 of Annex A.5.1 happens	<--	ACK	6	P
NOTE: The test procedure including NR/5GC signalling is specified in TS 38.508-1 [21] subclause 4.9.16.					

7.6.3.3 Specific message contents

None as fully described in annex A.5.1.

7.7 MTSI MT Voice Call without preconditions at both originating UE and terminating UE / 5GS

7.7.1 Test Purpose (TP)

(1)

```
with { UE being registered to IMS and configured to not use preconditions }
ensure that {
  when { UE receives INVITE for voice call }
    then { UE may respond with 100 Trying and then sends 183 Session Progress with SDP without
preconditions }
            }
```

(2)

```
with { UE having sent 183 Session Progress }
ensure that {
  when { UE receives PRACK for 183 Session Progress }
    then { UE sends 200 OK for PRACK }
            }
```

(3)

```
with { UE having sent 200 OK for PRACK }
ensure that {
  when { UE is ready to start the call }
    then { UE sends 180 Ringing followed by 200 OK for INVITE }
            }
```

7.7.2 Conformance Requirements

[TS 24.229, annex U.3.1.4]:

Upon receiving an INVITE request not including the "precondition" option-tag in the Supported header field and not including the "precondition" option-tag in the Require header field, and the IP-CAN performs network-initiated resource reservation for the UE, the UE:

1) if the INVITE request contains an SDP offer and the local resources required at the terminating UE for the received SDP offer are not available:

   a) shall not alert the user; and

   b) shall send 183 (Session Progress) response to the INVITE request without waiting for resource reservation and without alerting the user. If the INVITE request includes a Supported header field indicating support of reliable provisional responses, the UE shall send the 183 (Session Progress) response reliably. In the 183 (Session Progress) response, the UE shall include an SDP answer; and

2) if the INVITE request does not contain an SDP offer and the INVITE request includes a Supported header field indicating support of reliable provisional responses:

   a) shall generate an SDP offer;

   b) if the local resources required at the terminating UE for the generated SDP offer are not available:

      A) shall not alert the user; and

      B) shall reliably send 183 (Session Progress) response to the INVITE request without waiting for resource reservation and without alerting the user. In the 183 (Session Progress) response, the UE shall include the generated SDP offer.

Upon successful reservation of local resources, if the precondition mechanism is not used by the terminating UE, the UE can send 180 (Ringing) response to the INVITE request and can alert the user.

7.7.3 Test description

7.7.3.1 Pre-test conditions

System Simulator:

- 1 NR Cell connected to 5GC, default parameters.
- SS is configured to not use the precondition mechanism.

UE:

- UE contains either ISIM and USIM applications or only USIM application on UICC.
- UE is configured to register for IMS after switch on.

Preamble:

- The UE is in test state 1N-A (TS 38.508-1) and registered to IMS.

7.7.3.2 Test procedure sequence

Table 7.7.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	Step 1 of Annex A.5.2 happens	<--	INVITE		
2	Step 2 of Annex A.5.2 happens	-->	100 Trying		
3	Step 3 of Annex A.5.2 happens	-->	183 Session Progress	1	P
4	Step 4 of Annex A.5.2 happens	<--	PRACK		
5	Step 5 of Annex A.5.2 happens	-->	200 OK	2	P
6	Step 6 of Annex A.5.2 happens	-->	180 Ringing	3	P
7	Step 7 of Annex A.5.2 happens	<--	PRACK		
8	Step 8 of Annex A.5.2 happens	-->	200 OK		
9	Step 9 of Annex A.5.2 happens	-->	200 OK		
10	Step 10 of Annex A.5.2 happens	<--	ACK		
NOTE: The test procedure including NR/5GC signalling is specified in TS 38.508-1 [21] subclause 4.9.16.					

7.7.3.3 Specific message contents

None as fully described in annex A.5.2.

8 Supplementary Services

8.1 Originating Identification Presentation / Configuration / 5GS

8.1.1 Test Purpose (TP)

(1)

```
with { UE being registered to IMS }
ensure that {
  when { UE is made to activate OIP }
   then { UE authenticates itself using GBA }
            }
```

(2)

```
with { UE having started authentication using GBA }
ensure that {
  when { UE receives 200 OK concluding the authentication }
   then { UE sends HTTP request to activate OIP }
            }
```

(3)

```
with { UE having concluded activation of OIP }
ensure that {
  when { UE is made to de-activate OIP }
   then { UE sends HTTP request to de-activate OIP }
            }
```

8.1.2 Conformance Requirements

Generic requirements for Originating Identification Presentation can be found from TS 34.229-1 Annexes F.1 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.

[TS 24.109 clause 4.2]:

The UE shall initiate the bootstrapping procedure when:

a) the UE wants to interact with a NAF and bootstrapping is required;

b) a NAF has requested bootstrapping required indication as described in subclause 5.2.4 or bootstrapping renegotiation indication as described in subclause 5.2.5; or

c) the lifetime of the key has expired in the UE if one or more applications are using that key.

A UE and the BSF shall establish bootstrapped security association between them by running bootstrapping procedure. Bootstrapping security association consists of a bootstrapping transaction identifier (B-TID) and key material Ks.

Bootstrapping session on the BSF also includes security related information about subscriber (e.g. user's private identity). Bootstrapping session is valid for a certain time period, and shall be deleted in the BSF when the session becomes invalid.

Bootstrapping procedure shall be based on HTTP Digest AKA as described in 3GPP TS 33.220 [1] and in RFC 3310 [6] with the modifications described below.

The BSF address is derived from the IMPI or IMSI according to 3GPP TS 23.003 [7].

A UE shall indicate to the BSF that it supports the use of TMPI as defined in 3GPP 33.220 [1] by including a "product" token in the "User-Agent" header field (cf. RFC 2616 [14]) that is set to a static string "3gpp-gba-tmpi" in HTTP requests sent to the BSF.

A BSF shall indicate to the UE that it supports the use of TMPI as defined in 3GPP 33.220 [1] by including a "product" token in the "Server" header field (cf. RFC 2616 [14]) that is set to a static string "3gpp-gba-tmpi" in HTTP responses sent to the UE.

In the bootstrapping procedure, Authorization, WWW-Authenticate, and Authentication-Info HTTP headers shall be used as described in RFC 3310 [6] with following exceptions:

a) the "realm" parameter shall contain the network name where the username is authenticated;

b) the quality of protection ("qop") parameter shall be "auth-int"; and

c) the "username" parameter shall contain user's private identity (IMPI).

NOTE: If the UE does not have an ISIM application with an IMPI, the IMPI will be constructed from IMSI, according to 3GPP TS 23.003 [7].

In addition to RFC 3310 [6], the following apply:

a) In the initial request from the UE to the BSF, the UE shall include Authorization header with following parameters:

- the username directive, set to

1) the value of the TMPI if one has been associated with the private user identity as described in 3GPP 33.220 [1]; or

2) the value of the private user identity;

- the realm directive, set to the BSF address derived from the IMPI or IMSI according to 3GPP TS 23.003 [7];

- the uri directive, set to either absoluteURL "http://<BSF address>/" or abs_path "/", and which one is used is specified in RFC 2617 [9];

- the nonce directive, set to an empty value; and

- the response directive, set to an empty value;

b) In the challenge response from the BSF to the UE, the BSF shall include parameters to WWW-Authenticate header as specified in RFC 3310 [6] with following clarifications:

- the realm directive, set to the BSF address derived from the IMPI or IMSI according to 3GPP TS 23.003 [7];

c) In the message from the BSF to the UE, the BSF shall include bootstrapping transaction identifier (B-TID) and the key lifetime to an XML document in the HTTP response payload. The BSF may also include additional server specific data to the XML document. The XML schema definition of this XML document is given in Annex C.

d) When responding to a challenge from the BSF, the UE shall include an Authorization header containing a realm directive set to the value as received in the realm directive in the WWW-Authenticate header.

e) Authentication-Info header shall be included into the subsequent HTTP response after the BSF concluded that the UE has been authenticated. Authentication-Info header shall include the "rspauth" parameter.

After successful bootstrapping procedure the UE and the BSF shall contain the key material (Ks) and the B-TID. The key material shall be derived from AKA parameters as specified in 3GPP TS 33.220 [1]. In addition, BSF shall also contain a set of security specific attributes related to the UE.

An example flow of successful bootstrapping procedure can be found in clause A.3.

8.1.3 Test description

8.1.3.1 Pre-test conditions

System Simulator:

- SS is configured with 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 listening to SIP default port 5060 for both UDP and TCP protocols.
- At the SS, a HTTP Server is established at port 80 to simulate the XCAP server
- 1 NR Cell

UE:

- The 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.
- UE has activated an IPCAN bearer with SS.

Preamble:

- The UE is in test state 1N-A (TS 38.508-1) and registered to IMS.
- The UE has established a PDN connectivity for IMS XCAP signalling. The UE may either be configured to re-use the Internet APN for XCAP signalling or the UE uses a specific XCAP-only APN
- During these procedures the UE may request a DNS server address via NAS signalling and as parallel behaviour the UE may resolve the IP address of the XCAP server via DNS.

8.1.3.2 Test procedure sequence

Table 8.1.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	The UE is triggered for activation of OIP	-	-	-	-
2	Step 1 of TS 34.229-1 subclause C.29.2 happens	-->	HTTP Request	-	-
3	Step 2 of TS 34.229-1 subclause C.29.2 happens	<--	HTTP Response: 401 UNAUTHORIZED	-	-
4	Step 3 of TS 34.229-1 subclause C.29.2 happens Check: Does the UE send HTTP request with valid authorization credentials?	-->	HTTP Request	1	P
5	Step 4 of TS 34.229-1 subclause C.29.2 happens	<--	HTTP Response: 200 OK	-	-
6	Step 5 of TS 34.229-1 subclause C.29.1 happens	-	-		
7	Check: Does the Simservs document stored in the SS contain the following information supplied by UE? -<originating-identity-presentation> element with "active" attribute being set "true"	-	-	2	P
8	Make the UE attempt deactivation of OIP	-	-	-	-
9	Step 8 of TS 34.229-1 subclause C.29.1 happens	-	-	-	-
10	Check: Does the Simservs document stored in the SS contain the following information supplied by UE? -<originating-identity-presentation> element with "active" attribute being set "false"	-	-	3	P

8.1.3.3 Specific message contents

Table 8.1.3.3-1: HTTP Request and Responses (Table 8.1.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause C.29.1 and C.29.2

Editor's Note: XML content needs to be specified and refer to the HTTP steps once a generic procedure is defined.

8.2 to 8.17 FFS

8.18 Barring of All Incoming Calls / except for a specific user / 5GS

8.18.1 Test Purpose (TP)

(1)

```
with { UE being registered to IMS }
ensure that {
  when { UE is made to activate incoming communication barring except for a specific user (ICBESU) }
   then { UE authenticates itself using Digest }
            }
```

(2)

```
with { UE having started authentication using Digest }
ensure that {
  when { UE receives 200 OK concluding the authentication }
   then { UE sends HTTP request to activate ICBESU }
            }
```

(3)

```
with { UE having concluded activation of ICBESU }
ensure that {
  when { UE is made to de-activate ICBESU }
   then { UE sends HTTP request to de-activate ICBESU }
            }
```

8.18.2 Conformance Requirements

References: Conformance requirements for activating and deactivating Communication Barring are specified in TS 34.229-1 Annexes F.1 and F.5; TS 24.611, clause 4.9.1.4; TS 24.109, clause 4.2

[TS 24.611, clause 4.9.1.4]:

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.

[TS 24.109 clause 4.2]:

The UE shall initiate the bootstrapping procedure when:

a) the UE wants to interact with a NAF and bootstrapping is required;

b) a NAF has requested bootstrapping required indication as described in subclause 5.2.4 or bootstrapping renegotiation indication as described in subclause 5.2.5; or

c) the lifetime of the key has expired in the UE if one or more applications are using that key.

A UE and the BSF shall establish bootstrapped security association between them by running bootstrapping procedure. Bootstrapping security association consists of a bootstrapping transaction identifier (B-TID) and key material Ks. Bootstrapping session on the BSF also includes security related information about subscriber (e.g. user's private identity). Bootstrapping session is valid for a certain time period, and shall be deleted in the BSF when the session becomes invalid.

Bootstrapping procedure shall be based on HTTP Digest AKA as described in 3GPP TS 33.220 [1] and in RFC 3310 [6] with the modifications described below.

The BSF address is derived from the IMPI or IMSI according to 3GPP TS 23.003 [7].

A UE shall indicate to the BSF that it supports the use of TMPI as defined in 3GPP 33.220 [1] by including a "product" token in the "User-Agent" header field (cf. RFC 2616 [14]) that is set to a static string "3gpp-gba-tmpi" in HTTP requests sent to the BSF.

A BSF shall indicate to the UE that it supports the use of TMPI as defined in 3GPP 33.220 [1] by including a "product" token in the "Server" header field (cf. RFC 2616 [14]) that is set to a static string "3gpp-gba-tmpi" in HTTP responses sent to the UE.

In the bootstrapping procedure, Authorization, WWW-Authenticate, and Authentication-Info HTTP headers shall be used as described in RFC 3310 [6] with following exceptions:

a) the "realm" parameter shall contain the network name where the username is authenticated;

b) the quality of protection ("qop") parameter shall be "auth-int"; and

c) the "username" parameter shall contain user's private identity (IMPI).

NOTE: If the UE does not have an ISIM application with an IMPI, the IMPI will be constructed from IMSI, according to 3GPP TS 23.003 [7].

In addition to RFC 3310 [6], the following apply:

a) In the initial request from the UE to the BSF, the UE shall include Authorization header with following parameters:

- the username directive, set to

1) the value of the TMPI if one has been associated with the private user identity as described in 3GPP 33.220 [1]; or

2) the value of the private user identity;

- the realm directive, set to the BSF address derived from the IMPI or IMSI according to 3GPP TS 23.003 [7];

- the uri directive, set to either absoluteURL "http://<BSF address>/" or abs_path "/", and which one is used is specified in RFC 2617 [9];

- the nonce directive, set to an empty value; and

- the response directive, set to an empty value;

b) In the challenge response from the BSF to the UE, the BSF shall include parameters to WWW-Authenticate header as specified in RFC 3310 [6] with following clarifications:

- the realm directive, set to the BSF address derived from the IMPI or IMSI according to 3GPP TS 23.003 [7];

c) In the message from the BSF to the UE, the BSF shall include bootstrapping transaction identifier (B-TID) and the key lifetime to an XML document in the HTTP response payload. The BSF may also include additional server specific data to the XML document. The XML schema definition of this XML document is given in Annex C.

d) When responding to a challenge from the BSF, the UE shall include an Authorization header containing a realm directive set to the value as received in the realm directive in the WWW-Authenticate header.

e) Authentication-Info header shall be included into the subsequent HTTP response after the BSF concluded that the UE has been authenticated. Authentication-Info header shall include the "rspauth" parameter.

After successful bootstrapping procedure the UE and the BSF shall contain the key material (Ks) and the B-TID. The key material shall be derived from AKA parameters as specified in 3GPP TS 33.220 [1]. In addition, BSF shall also contain a set of security specific attributes related to the UE.

An example flow of successful bootstrapping procedure can be found in clause A.3.

8.18.3 Test description

8.18.3.1 Pre-test conditions

System Simulator:

- SS is configured 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 listening to SIP default port 5060 for both UDP and TCP protocols.
- At the SS, a HTTP Server is established at port 80 to simulate the XCAP server
- 1 NR Cell

UE:

- 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.
- UE has activated an IPCAN bearer with SS.

Preamble:

- The UE is in test state 1N-A (TS 38.508-1) and registered to IMS
- The UE has established a PDN connectivity for IMS XCAP signalling. The UE may either be configured to re-use the Internet APN for XCAP signalling or the UE uses a specific XCAP-only APN
- During these procedures the UE may request a DNS server address via NAS signalling and as parallel behaviour the UE may resolve the IP address of the XCAP server via DNS.

8.18.3.2 Test procedure sequence

Table 8.18.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	UE is triggered for activation of supplementary service ICBESU	-	-	-	-
2	UE sends Initial HTTP Request (Note 1)	-->	HTTP Request		
	EXCEPTION: steps 3 and 4 describe behaviour in case of HTTP Digest XCAP authentication when the UE does not provide correct authorization credentials within its initial request	-	-	-	-
3	SS sends HTTP Response: “401 Unauthorized”	<--	HTTP Response: 401 Unauthorized	-	-
4	Check: Does the UE send HTTP Request with valid authorization credentials?	-->	HTTP Request	1	P
5	SS sends HTTP Response: “200 OK”	<--	HTTP Response: 200 OK	-	-
	EXCEPTION: Steps 6 and steps 7 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	-	-	-	-
6	Check: Does the UE send HTTP Request? (Note 1)	-->	HTTP Request	2	P
7	SS sends HTTP Response: “200 OK” or “404 File Not Found” (Note 2)	<--	HTTP Response	-	-
8	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)	-	-
9	UE is triggered for deactivation of supplementary service ICBESU	-	-	-	-
	EXCEPTION: steps 10 and 11 describe the 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	-	-	-	-
10	Check: Does the UE send HTTP Request? (Note 1)	-->	HTTP Request	3	P
11	SS sends HTTP Response: “200 OK” or “404 File Not Found” (Note 2)	<--	HTTP Response	-	-
12	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: “404 File Not Found” is sent as response for a GET request to a non-existing node.					

8.18.3.3 Specific message contents

Table 8.18.3.3-1: HTTP Requests and Responses (Table 8.18.3.2-1)

Derivation Path: TS 34.229-1 [2], Tables in subclause C.29.1 and C.29.2

Editor's Note: XML content needs to be specified and refer to the HTTP steps once a generic procedure is defined.

9. SMS

9.1 Mobile Originating SMS / 5GS

9.1.1 Test Purpose (TP)

(1)

```
with { UE being registered to IMS }
ensure that {
  when { UE is made to send an SMS over IP }
    then { UE sends a SIP MESSAGE request containing a short message }
            }
```

(2)

```
with { UE having sent a SIP MESSAGE request containing a short message }
ensure that {
  when { UE receives a 202 Accepted response, followed by a SIP MESSAGE request containing a
submission report  }
    then { UE sends a 200 OK response }
            }
```

(3)

```
with { UE having sent a 200 OK response for submission report }
ensure that {
  when { UE receives a SIP MESSAGE request containing a status report }
    then { UE sends a 200 OK response, followed by a SIP MESSAGE request containing a delivery
report for status report }
            }
```

9.1.2 Conformance Requirements

[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[14], clauses 5.3.1.2, 5.3.1.3 and 5.3.2.4.

9.1.3 Test description

9.1.3.1 Pre-test conditions

System Simulator:

- 1 NR Cell connected to 5GC, default parameters.

UE:

- UE contains either ISIM and USIM applications or only USIM application on UICC.
- UE is configured to register for IMS after switch on.

Preamble:

- The UE is in test state 1N-A (TS 38.508-1) and registered to IMS.

9.1.3.2 Test procedure sequence

Table 9.1.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	UE is made to attempt a Mobile Originating SMS over IMS	-	-	-	-
2	Check: Does UE send a SIP MESSAGE request including a vnd.3gpp.sms payload that contains a short message?	-->	SIP MESSAGE	1	P
3	SS responds with 202 Accepted	<--	202 Accepted	-	-
4	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	<--	SIP MESSAGE	-	-
5	UE responds with 200 OK	-->	200 OK	2	P
6	SS sends a SIP MESSAGE request including a vnd.3gpp.sms payload that contains a status report	<--	SIP MESSAGE	-	-
7	Check: Does UE respond with 200 OK?	-->	200 OK	3	P
8	Check: Does UE send a SIP MESSAGE request including a vnd.3gpp.sms payload that contains a delivery report for the status report received at Step 6?	-->	SIP MESSAGE	3	P
9	SS responds with 202 Accepted	<--	202 Accepted	-	-
NOTE: The test procedure including NR/5GC signalling is specified in TS 38.508-1 [21] subclause FFS.					

9.1.3.3 Specific message contents

Table 9.1.3.3-1: SIP MESSAGE (step 2, table 9.1.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.7.3, Condition A5

Table 9.1.3.3-2: 202 Accepted (step 3 and 9, table 9.1.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.3.3

Table 9.1.3.3-3: SIP MESSAGE (step 4, table 9.1.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.7.4

Table 9.1.3.3-4: 200 OK (step 5 and 7, table 9.1.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.3.1, Condition A5 and A22

Table 9.1.3.3-5: SIP MESSAGE (step6, table 9.1.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.7.5

Table 9.1.3.3-6: SIP MESSAGE (step 8, table 9.1.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.7.6

9.2 Mobile Originating SMS / 5GS

9.2.1 Test Purpose (TP)

(1)

```
with { UE being registered to IMS }
ensure that {
  when { UE receives a SIP MESSAGE request containing a short message }
    then { UE sends a 200 OK response, followed by a SIP MESSAGE request containing a delivery
report }
            }
```

9.2.2 Conformance Requirements

[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[14], clause 5.3.2.3 and 5.3.2.4.

9.2.3 Test description

9.2.3.1 Pre-test conditions

System Simulator:

- 1 NR Cell connected to 5GC, default parameters.

UE:

- UE contains either ISIM and USIM applications or only USIM application on UICC.
- UE is configured to register for IMS after switch on.

Preamble:

- The UE is in test state 1N-A (TS 38.508-1) and registered to IMS.

9.2.3.2 Test procedure sequence

Table 9.2.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	The SS sends a Short Message.	<--	SIP MESSAGE	-	-
2	Check: Does the UE respond with 200 OK?	-->	200 OK	1	P
3	Check: Does the UE respond a delivery report?	-->	SIP MESSAGE	1	P
4	The SS sends an accepted response.	<--	202 ACCEPTED	-	-
NOTE: The test procedure including NR/5GC signalling is specified in TS 38.508-1 [21] subclause FFS.					

9.2.3.3 Specific message contents

Table 9.2.3.3-1: SIP MESSAGE (step 1, table 9.2.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.7.1

Table 9.2.3.3-2: 200 OK (step 2 table 9.2.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.3.1, Condition A5 and A22

Table 9.2.3.3-3: SIP MESSAGE (step 3, table 9.2.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.7.2

Table 9.2.3.3-4: 202 Accepted (step 4, table 9.2.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.3.3

9.3 Mobile Originating Concatenated SMS / 5GS

9.3.1 Test Purpose (TP)

(1)

```
with { UE being registered to IMS }
ensure that {
  when { UE is made to send a concatenated SMS over IP }
   then { UE sends a SIP MESSAGE request containing the first segment of the concatenated SMS }
            }
```

(2)

```
with { UE having sent a SIP MESSAGE request containing the first segment of the concatenated SMS }
ensure that {
  when { UE receives a 202 Accepted response, followed by a SIP MESSAGE request containing a
submission report for the first segment }
   then { UE sends a 200 OK response, followed by a SIP MESSAGE request containing the second
segment of the concatenated SMS }
            }
```

(3)

```
with { UE having sent a SIP MESSAGE request containing the second segment of the concatenated SMS }
ensure that {
  when { UE receives a 202 Accepted response, followed by a SIP MESSAGE request containing a
submission report for the second segment }
   then { UE sends a 200 OK response, followed by a SIP MESSAGE request containing the third segment
of the concatenated SMS }
            }
```

(4)

```
with { UE having sent a SIP MESSAGE request containing the third segment of the concatenated SMS }
ensure that {
  when { UE receives a 202 Accepted response, followed by a SIP MESSAGE request containing a
submission report for the third segment }
   then { UE sends a 200 OK response }
            }
```

9.3.2 Conformance Requirements

References: The conformance requirements covered in the present TC are specified in TS 23.040, clause 9.2.3.23; TS 24.341, clause 5.3.2.3 and TS 24.341, clause 5.3.2.4.

[TS 23.040, clause 9.2.3.23]:

The TP-User-Data-Header-Indicator is a 1 bit field within bit 6 of the first octet of the following six PDUs:

- SMS-SUBMIT,
- SMS-SUBMIT-REPORT,
- SMS-DELIVER,
- SMS-DELIVER-REPORT,
- SMS-STATUS-REPORT,
- SMS-COMMAND.

TP-UDHI has the following values.

Bit no. 6 0 The TP-UD field contains only the short message

1 The beginning of the TP-UD field contains a Header in addition to the short message.

[TS 23.040, clause 9.2.3.24]:

The length of the TP-User-Data field is defined in the PDU's of the SM-TL (see clause 9.2.2).

The TP-User-Data field may comprise just the short message itself or a Header in addition to the short message depending upon the setting of TP-UDHI.

Where the TP-UDHI value is set to 0 the TP-User-Data field comprises the short message only, where the user data can be 7 bit (default alphabet) data, 8 bit data, or 16 bit (UCS2 [24]) data.

Where the TP-UDHI value is set to 1 the first octets of the TP-User-Data field contains a Header in the following order starting at the first octet of the TP-User-Data field.

Irrespective of whether any part of the User Data Header is ignored or discarded, the MS shall always store the entire TPDU exactly as received.

FIELD	LENGTH
Length of User Data Header	1 octet
Information-Element-Identifier "A"	1 octet
Length of Information-Element "A"	1 octet
Information-Element "A" Data	0 to "n" octets
Information-Element-Identifier "B"	1 octet
Length of Information-Element "B"	1 octet
Information-Element "B" Data	0 to "n" octets
Information-Element-Identifier "X"	1 octet
Length of Information-Element "X"	1 octet
Information-Element "X" Data	0 to "n" octets

The diagram below shows the layout of the TP-User-Data-Length and the TP-User-Data for uncompressed GSM 7 bit default alphabet data. The UDHL field is the first octet of the TP-User-Data content of the Short Message.

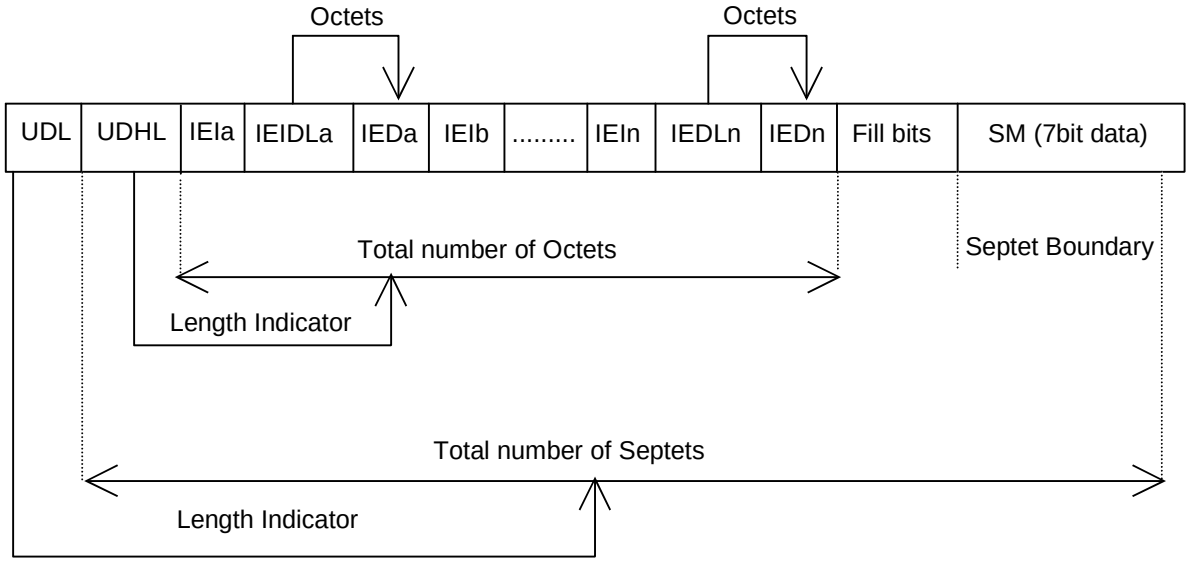

Figure 9.2.3.24 (a)

The diagram below shows the layout of the TP-User-Data-Length and the TP-User-Data for uncompressed 8 bit data or uncompressed UCS2 data. The UDHL field is the first octet of the TP-User-Data content of the Short Message.

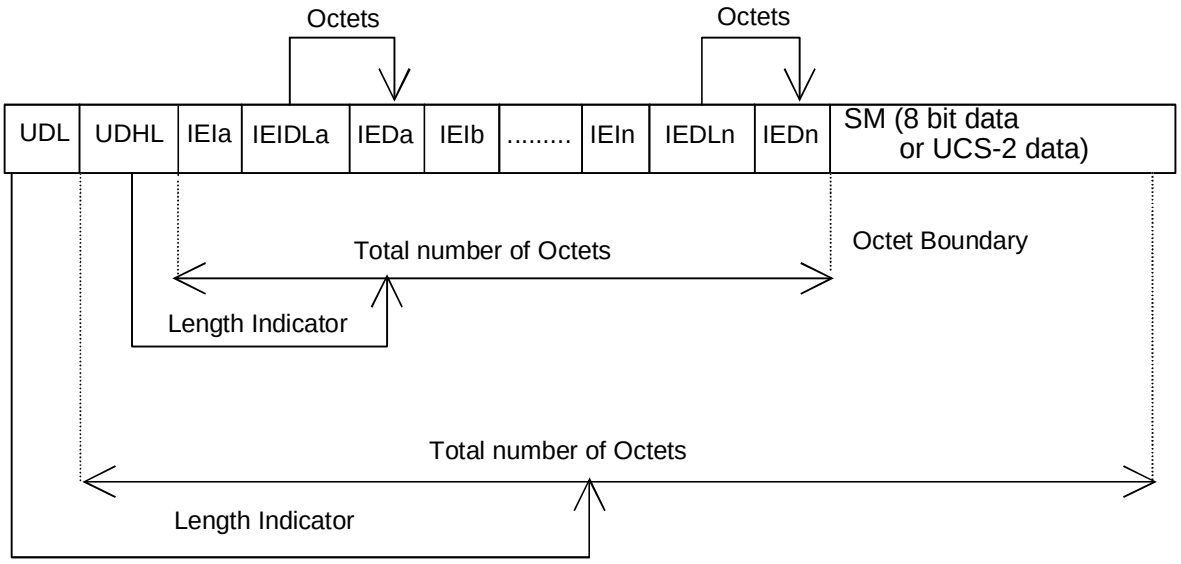

Figure 9.2.3.24 (b)

The diagram below shows the layout of the TP-User-Data-Length and the TP-User-Data for compressed GSM 7 bit default alphabet data, compressed 8 bit data or compressed UCS2 data. The UDHL field is the first octet of the TP-User-Data content of the Short Message.

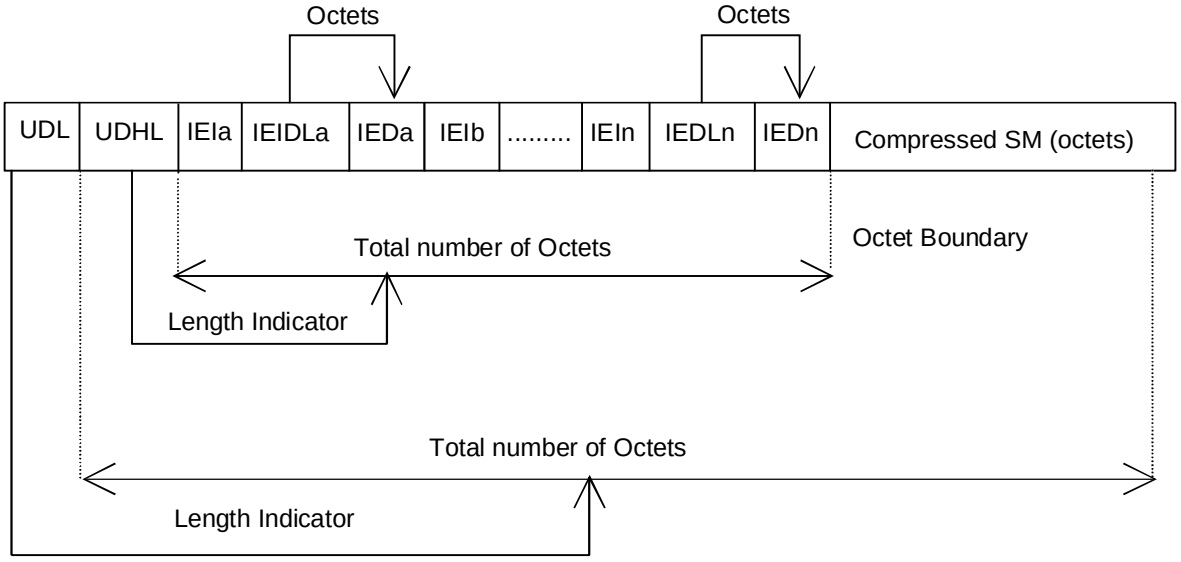

Figure 9.2.3.24 (c)

The definition of the TP-User-Data-Length field which immediately precedes the "Length of User Data Header" is unchanged and shall therefore be the total length of the TP-User-Data field including the Header, if present. (see 9.2.3.16).

The "Length-of-Information-Element" fields shall be the integer representation of the number of octets within its associated "Information-Element-Data" field which follows and shall not include itself in its count value.

The "Length-of-User-Data-Header" field shall be the integer representation of the number of octets within the "User-Data-Header" information fields which follow and shall not include itself in its count or any fill bits which may be present (see text below).

Information Elements may appear in any order and need not follow the order used in the present document. Information Elements are classified into 3 categories as described below.

- SMS Control – identifies those IEIs which have the capability of dictating SMS functionality.
- EMS Control – identifies those IEIs which manage EMS Content IEIs.
- EMS Content – identifies those IEIs containing data of a unique media format.

It is permissible for certain IEs to be repeated within a short message, or within a concatenated message. There is no restriction on the repeatability of IEs in the EMS Content classification. The repeatability of SMS Control and EMS Control IEs is determined on an individual basis. See the IE table below for the repeatability of each IE.

In the event that IEs determined as not repeatable are duplicated, the last occurrence of the IE shall be used. In the event that two or more IEs occur which have mutually exclusive meanings (e.g. an 8bit port address and a 16bit port address), then the last occurring IE shall be used.

If the length of the User Data Header is such that there are too few or too many octets in the final Information Element then the whole User Data Header shall be ignored.

If any reserved values are received within the content of any Information Element then that part of the Information Element shall be ignored.

The support of any Information Element Identifier is optional unless otherwise stated.

The Information Element Identifier octet shall be coded as follows:

VALUE (hex)	MEANING	Classification	Repeatability
00	Concatenated short messages, 8-bit reference number	SMS Control	No
01	Special SMS Message Indication	SMS Control	Yes
02	Reserved	N/A	N/A
03	Value not used to avoid misinterpretation as <LF> character	N/A	N/A
04	Application port addressing scheme, 8 bit address	SMS Control	No
05	Application port addressing scheme, 16 bit address	SMS Control	No
06	SMSC Control Parameters	SMS Control	No
07	UDH Source Indicator	SMS Control	Yes
08	Concatenated short message, 16-bit reference number	SMS Control	No
09	Wireless Control Message Protocol	SMS Control	Note 3
0A	Text Formatting	EMS Control	Yes
0B	Predefined Sound	EMS Content	Yes
0C	User Defined Sound (iMelody max 128 bytes)	EMS Content	Yes
0D	Predefined Animation	EMS Content	Yes
0E	Large Animation (16*16 times 4 = 32*4 =128 bytes)	EMS Content	Yes
0F	Small Animation (8*8 times 4 = 8*4 =32 bytes)	EMS Content	Yes
10	Large Picture (32*32 = 128 bytes)	EMS Content	Yes
11	Small Picture (16*16 = 32 bytes)	EMS Content	Yes
12	Variable Picture	EMS Content	Yes
13	User prompt indicator	EMS Control	Yes
14	Extended Object	EMS Content	Yes
15	Reused Extended Object	EMS Control	Yes
16	Compression Control	EMS Control	No
17	Object Distribution Indicator	EMS Control	Yes
18	Standard WVG object	EMS Content	Yes
19	Character Size WVG object	EMS Content	Yes
1A	Extended Object Data Request Command	EMS Control	No
1B-1F	Reserved for future EMS features (see subclause 3.10)	N/A	N/A
20	RFC 5322 E-Mail Header	SMS Control	No
21	Hyperlink format element	SMS Control	Yes
22	Reply Address Element	SMS Control	No
23	Enhanced Voice Mail Information	SMS Control	No
24	National Language Single Shift	SMS Control	No
25	National Language Locking Shift	SMS Control	No
26 – 6F	Reserved for future use	N/A	N/A
70 – 7F	(U)SIM Toolkit Security Headers	SMS Control	Note 1
80 – 9F	SME to SME specific use	SMS Control	Note 2
A0 – BF	Reserved for future use	N/A	N/A
C0 – DF	SC specific use	SMS Control	Note 2
E0 – FF	Reserved for future use	N/A	N/A

Note 1: The functionality of these IEIs is defined in 3GPP TSG 31.115 [28], and therefore, the repeatability is not within the scope of this document and will not be determined here.

Note 2: The functionality of these IEIs is used in a proprietary fashion by different SMSC vendors, and therefore, are not within the scope of this technical specification.

Note 3: The functionality of these IEIs is defined by the WAP Forum and therefore the repeatability is not within the scope of this document and will not be determined here.

A receiving entity shall ignore (i.e. skip over and commence processing at the next information element) any information element where the IEI is Reserved or not supported. The receiving entity calculates the start of the next information element by looking at the length of the current information element and skipping that number of octets.

The SM itself may be coded as 7, 8 or 16 bit data.

If 7 bit data is used and the TP-UD-Header does not finish on a septet boundary then fill bits are inserted after the last Information Element Data octet up to the next septet boundary so that there is an integral number of septets for the entire TP-UD header. This is to ensure that the SM itself starts on an septet boundary so that an earlier Phase mobile shall be capable of displaying the SM itself although the TP-UD Header in the TP-UD field may not be understood.

It is optional to make the first character of the SM itself a Carriage Return character encoded according to the default 7 bit alphabet so that earlier Phase mobiles, which do not understand the TP-UD-Header, shall over-write the displayed TP-UD-Header with the SM itself.

If 16 bit (USC2) data is used then padding octets are not necessary. The SM itself shall start on an octet boundary.

If 8 bit data is used then padding is not necessary. An earlier Phase mobile shall be able to display the SM itself although the TP-UD header may not be understood.

It is also possible for mobiles not wishing to support the TP-UD header to check the value of the TP-UDHI bit in the SMS-Deliver PDU and the first octet of the TP-UD field and skip to the start of the SM and ignore the TP-UD header.

[TS 23.040, clause 9.2.3.24.1]:

This facility allows short messages to be concatenated to form a longer message.

In the case of uncompressed 8-bit data, the maximum length of the short message within the TP-UD field is 134 (140-6) octets.

In the case of uncompressed GSM 7 bit default alphabet data, the maximum length of the short message within the TP-UD field is 153 (160-7) characters. A character represented by an escape-sequence shall not be split in the middle.

In the case of 16 bit uncompressed USC2 data, the maximum length of the short message within the TP-UD field is 67 ((140-6)/2) characters. A UCS2 character shall not be split in the middle; if the length of the User Data Header is odd, the maximum length of the whole TP-UD field is 139 octets.

In the case of compressed GSM 7 bit default alphabet data, 8 bit data or UCS2 the maximum length of the compressed short message within the TP-UD field is 134 (140-6) octets including the Compression Header and Compression Footer, both or either of which may be present (see clause 3.9).

The maximum length of an uncompressed concatenated short message is 39015 (255*153) default alphabet characters, 34170 (255*134) octets or 17085 (255*67) UCS2 characters.

The maximum length of a compressed concatenated message is 34170 (255*134) octets including the Compression Header and Compression Footer (see clause 3.9 and figure 9.2.3.24.1(a) below).

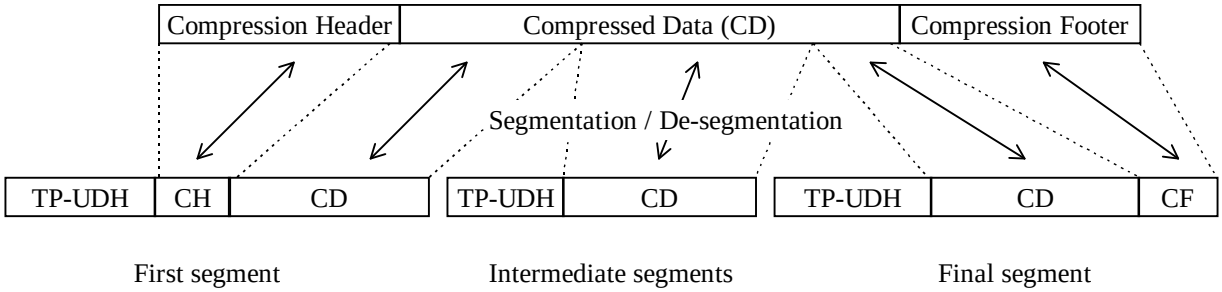

Figure 9.2.3.24.1 (a): Concatenation of a Compressed short message

The Information-Element-Data field contains information set by the application in the SMS-SUBMIT so that the receiving entity is able to re-assemble the short messages in the correct order. Each concatenated short message contains a reference number which together with the originating address and Service Centre address allows the receiving entity to discriminate between concatenated short messages sent from different originating SMEs and/or SCs. In a network which has multiple SCs, it is possible for different segments of a concatenated SM to be sent via different SCs and so it is recommended that the SC address should not be checked by the MS unless the application specifically requires such a check.

The TP elements in the SMS-SUBMIT PDU, apart from TP-MR, TP-SRR, TP-UDL and TP-UD, should remain unchanged for each SM which forms part of a concatenated SM, otherwise this may lead to irrational behaviour. TP-MR must be incremented for every segment of a concatenated message as defined in clause 9.2.3.6. A SC shall handle segments of a concatenated message like any other short message. The relation between segments of a concatenated message is made only at the originator, where the message is segmented, and at the recipient, where the message is reassembled. SMS-COMMANDs identify messages by TP-MR and therefore apply to only one segment of a

concatenated message. It is up to the originating SME to issue SMS-COMMANDs for all the required segments of a concatenated message.

The Information-Element-Data octets shall be coded as follows.

Octet 1 Concatenated short message reference number.

This octet shall contain a modulo 256 counter indicating the reference number for a particular concatenated short message. This reference number shall remain constant for every short message which makes up a particular concatenated short message.

Octet 2 Maximum number of short messages in the concatenated short message.

This octet shall contain a value in the range 0 to 255 indicating the total number of short messages within the concatenated short message. The value shall start at 1 and remain constant for every short message which makes up the concatenated short message. If the value is zero then the receiving entity shall ignore the whole Information Element.

Octet 3 Sequence number of the current short message.

This octet shall contain a value in the range 0 to 255 indicating the sequence number of a particular short message within the concatenated short message. The value shall start at 1 and increment by one for every short message sent within the concatenated short message. If the value is zero or the value is greater than the value in octet 2 then the receiving entity shall ignore the whole Information Element.

The IEI and associated IEI length and IEI data shall be present in every segment of the concatenated SM.

[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.

9.3.3 Test description

9.3.3.1 Pre-test conditions

System Simulator:

- 1 NR Cell connected to 5GC, default parameters.

UE:

- UE contains either ISIM and USIM applications or only USIM application on UICC.
- UE is configured to register for IMS after switch on.
- SMS over IP is enabled.

Preamble:

- The UE is in test state 1N-A (TS 38.508-1 [21]) and registered to IMS.

9.3.3.2 Test procedure sequence

Table 9.3.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	UE is made to send a Concatenated SMS over IP (The length of SMS text is determined so that the amount of segments of the concatenated SMS is three).	-	-	-	-
2	Check: Does the UE send a SIP MESSAGE request including a vnd.3gpp.sms payload that contains the first segment of the concatenated SMS?	-->	SIP MESSAGE request	1	P
3	SS responds with 202 Accepted.	<--	202 Accepted	-	-
4	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 first segment of the concatenated SMS sent by the UE at Step 1.	<--	SIP MESSAGE request	-	-
5	UE responds with 200 OK.	-->	200 OK	2	P
6	Check: Does the UE send a SIP MESSAGE request including a vnd.3gpp.sms payload that contains the second segment of the concatenated SMS?	-->	SIP MESSAGE request	2	P
7	SS responds with 202 Accepted.	<--	202 Accepted	-	-
8	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 second segment of the concatenated SMS sent by the UE at Step 5.	<--	SIP MESSAGE request	-	-
9	UE responds with 200 OK.	-->	200 OK	3	P
10	Check: Does the UE send a SIP MESSAGE request including a vnd.3gpp.sms payload that contains the final segment of the concatenated SMS?	-->	SIP MESSAGE request	3	P
11	SS responds with 202 Accepted.	<--	202 Accepted	-	-
12	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 final segment of the concatenated SMS sent by the UE at Step 9.	<--	SIP MESSAGE request	-	-
13	Check: Does the UE respond with 200 OK?	-->	200 OK	4	P

9.3.3.3 Specific message contents

Table 9.3.3.3-1: MESSAGE for MO SMS (step 1, table 9.3.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in annex A.7.3				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Message-body		- TP-UDHI='1'B (The beginning of the TP UD field contains a Header in addition to the short message.) - TP-MR=any allowed value - TP-UD - Length of User Data Header (UDHL)=5 - Information Element Identifier (IEI)=0x00 (Concatenated short messages, 8-bit reference number) - Length of Information Element (IEIDL)=3 - Concatenated short message reference number=any allowed value - Maximum number of short messages in the concatenated short message=3 - Sequence number of the current short message=1		TS 24.011 [25] TS 23.040 [24]

Table 9.3.3.3-2: 202 ACCEPTED (step 2, table 9.3.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.3.3

Table 9.3.3.3-3: Short message submission report for MO SMS (step 3, table 9.3.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in annex A.7.4				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Message-body		RP-ERROR message with RP-Cause Data: Length: 2, Length indicator = 1 Extension: not extended Cause value: 38 (Network out of order)		TS 24.011 [25] TS 23.040 [24]

Table 9.3.3.3-4: 200 OK for other requests than REGISTER or SUBSCRIBE (step 4, table 9.3.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.3.1, Condition A5, A22

Table 9.3.3.3-5: MESSAGE for MO SMS (step 5, table 9.3.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in annex A.7.3				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Message-body		- TP-UDHI='1'B (The beginning of the TP UD field contains a Header in addition to the short message.) - TP-MR= The value sent in the step1 + 1 (incremented) - TP-UD - Length of User Data Header (UDHL)=5 - Information Element Identifier (IEI)=0x00 (Concatenated short messages, 8-bit reference number) - Length of Information Element (IEIDL)=3 - Concatenated short message reference number= The same value sent in the step1 - Maximum number of short messages in the concatenated short message=3 - Sequence number of the current short message=2		TS 24.011 [25] TS 23.040 [24]

Table 9.3.3.3-6: 202 ACCEPTED (step 6, table 9.3.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.3.3

Table 9.3.3.3-7: Short message submission report for MO SMS (step 7, table 9.3.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in annex A.7.4				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Message-body		RP-ERROR message with RP-Cause Data: Length: 2, Length indicator = 1 Extension: not extended Cause value: 38 (Network out of order)		TS 24.011 [25] TS 23.040 [24]

Table 9.3.3.3-8: 200 OK for other requests than REGISTER or SUBSCRIBE (step 8, table 9.3.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.3.1, Condition A5, A22

Table 9.3.3.3-9: MESSAGE for MO SMS (step 9, table 9.3.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in annex A.7.3				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Message-body		- TP-UDHI='1'B (The beginning of the TP UD field contains a Header in addition to the short message.) - TP-MR= The value sent in the step5 + 1 (incremented) - TP-UD - Length of User Data Header (UDHL)=5 - Information Element Identifier (IEI)=0x00 (Concatenated short messages, 8-bit reference number) - Length of Information Element (IEIDL)=3 - Concatenated short message reference number= The same value sent in the step5 - Maximum number of short messages in the concatenated short message=3 - Sequence number of the current short message=3		TS 24.011 [25] TS 23.040 [24]

Table 9.3.3.3-10: 202 ACCEPTED (step 10, table 9.3.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.3.3

Table 9.3.3.3-11: Short message submission report for MO SMS (step 11, table 9.3.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in annex A.7.4				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Message-body		RP-ERROR message with RP-Cause Data: Length: 2, Length indicator = 1 Extension: not extended Cause value: 38 (Network out of order)		TS 24.011 [25] TS 23.040 [24]

Table 9.3.3.3-12: 200 OK for other requests than REGISTER or SUBSCRIBE (step 12, table 9.3.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.3.1, Condition A5, A22

9.4 Mobile Terminating Concatenated SMS / 5GS

9.4.1 Test Purpose (TP)

(1)

```
with { UE being registered to IMS }
ensure that {
  when { UE receives a SIP MESSAGE request containing a first segment of a concatenated SMS }
then { UE sends a 200 OK response, followed by a SIP MESSAGE request containing a delivery report
for the first segment }
    }
```

(2)

```
with { UE having sent a SIP MESSAGE request containing a delivery report for the first segment }
ensure that {
  when { UE receives a 202 Accepted response, followed by a SIP MESSAGE request containing a second
segment of a concatenated SMS }
    then { UE sends a 200 OK response, followed by a SIP MESSAGE request containing a delivery
report for the second segment }
    }
```

(3)

```
with { UE having sent a SIP MESSAGE request containing a delivery report for the second segment }
ensure that {
  when { UE receives a 202 Accepted response, followed by a SIP MESSAGE request containing a third
segment of a concatenated SMS }
    then { UE sends a 200 OK response, followed by a SIP MESSAGE request containing a delivery
report for the third segment }
    }
```

9.4.2 Conformance Requirements

[TS 23.040, clause 9.2.3.23]:

The TP-User-Data-Header-Indicator is a 1 bit field within bit 6 of the first octet of the following six PDUs:

- SMS-SUBMIT,
- SMS-SUBMIT-REPORT,
- SMS-DELIVER,
- SMS-DELIVER-REPORT,
- SMS-STATUS-REPORT,
- SMS-COMMAND.

TP-UDHI has the following values.

Bit no. 6 0 The TP-UD field contains only the short message

1 The beginning of the TP-UD field contains a Header in addition to the short message.

[TS 23.040, clause 9.2.3.24]:

The length of the TP-User-Data field is defined in the PDU's of the SM-TL (see clause 9.2.2).

The TP-User-Data field may comprise just the short message itself or a Header in addition to the short message depending upon the setting of TP-UDHI.

Where the TP-UDHI value is set to 0 the TP-User-Data field comprises the short message only, where the user data can be 7 bit (default alphabet) data, 8 bit data, or 16 bit (UCS2 [24]) data.

Where the TP-UDHI value is set to 1 the first octets of the TP-User-Data field contains a Header in the following order starting at the first octet of the TP-User-Data field.

Irrespective of whether any part of the User Data Header is ignored or discarded, the MS shall always store the entire TPDU exactly as received.

FIELD	LENGTH
Length of User Data Header	1 octet
Information-Element-Identifier "A"	1 octet
Length of Information-Element "A"	1 octet
Information-Element "A" Data	0 to "n" octets
Information-Element-Identifier "B"	1 octet
Length of Information-Element "B"	1 octet
Information-Element "B" Data	0 to "n" octets
Information-Element-Identifier "X"	1 octet
Length of Information-Element "X"	1 octet
Information-Element "X" Data	0 to "n" octets

The diagram below shows the layout of the TP-User-Data-Length and the TP-User-Data for uncompressed GSM 7 bit default alphabet data. The UDHL field is the first octet of the TP-User-Data content of the Short Message.

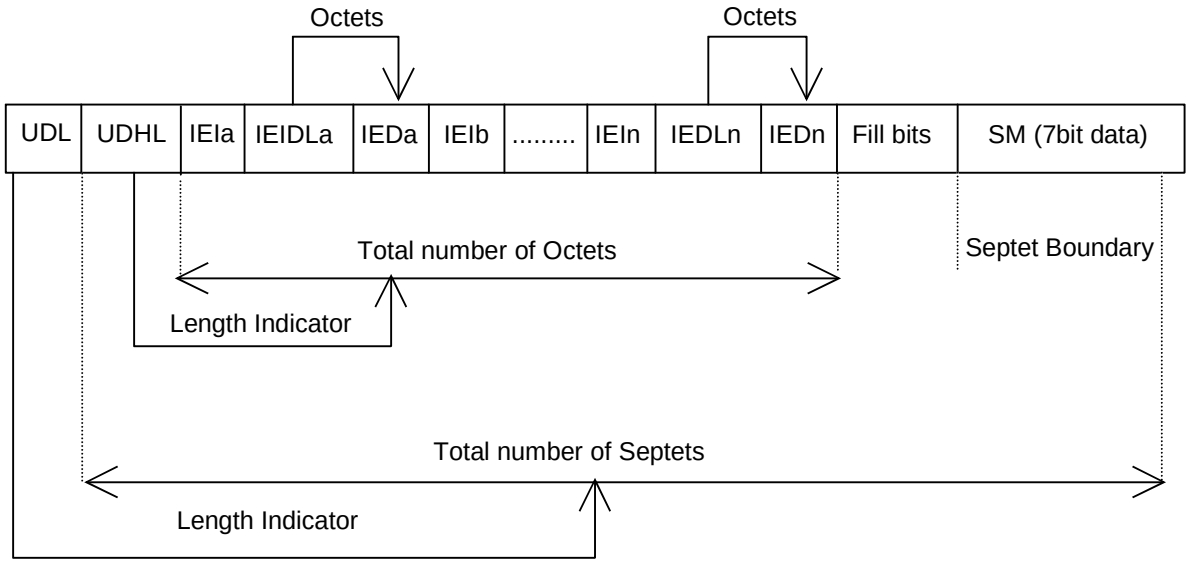

Figure 9.2.3.24 (a)

The diagram below shows the layout of the TP-User-Data-Length and the TP-User-Data for uncompressed 8 bit data or uncompressed UCS2 data. The UDHL field is the first octet of the TP-User-Data content of the Short Message.

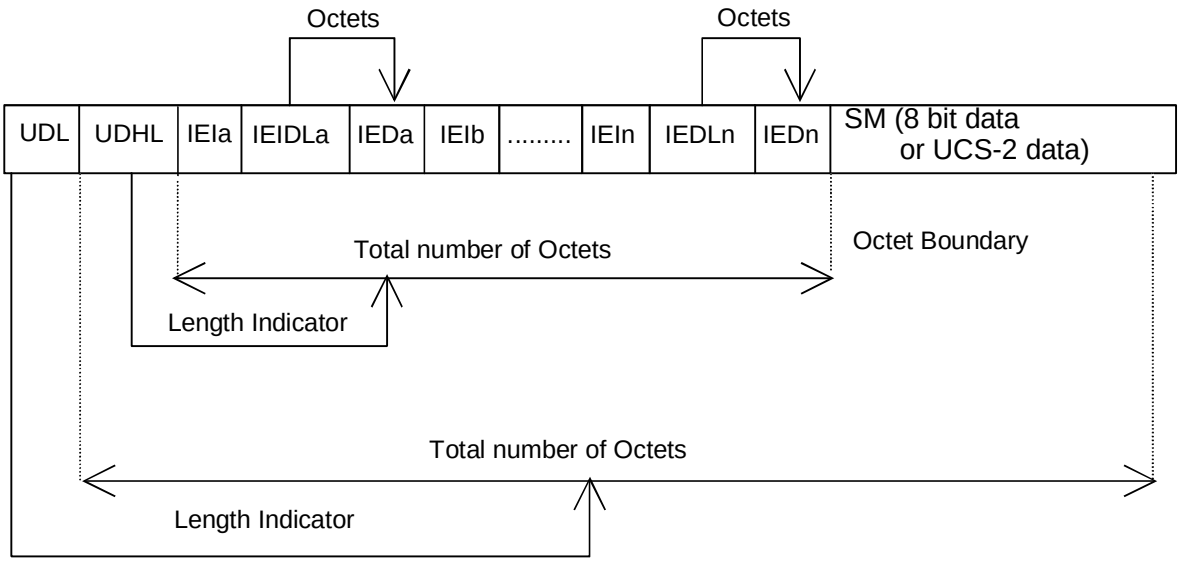

Figure 9.2.3.24 (b)

The diagram below shows the layout of the TP-User-Data-Length and the TP-User-Data for compressed GSM 7 bit default alphabet data, compressed 8 bit data or compressed UCS2 data. The UDHL field is the first octet of the TP-User-Data content of the Short Message.

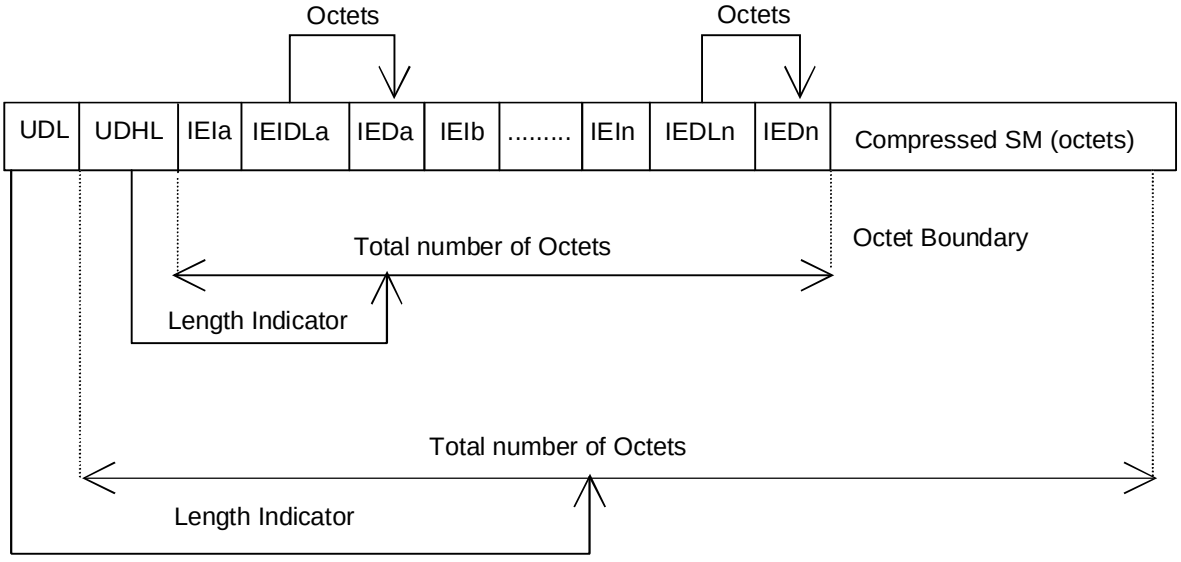

Figure 9.2.3.24 (c)

The definition of the TP-User-Data-Length field which immediately precedes the "Length of User Data Header" is unchanged and shall therefore be the total length of the TP-User-Data field including the Header, if present. (see 9.2.3.16).

The "Length-of-Information-Element" fields shall be the integer representation of the number of octets within its associated "Information-Element-Data" field which follows and shall not include itself in its count value.

The "Length-of-User-Data-Header" field shall be the integer representation of the number of octets within the "User-Data-Header" information fields which follow and shall not include itself in its count or any fill bits which may be present (see text below).

Information Elements may appear in any order and need not follow the order used in the present document. Information Elements are classified into 3 categories as described below.

- SMS Control – identifies those IEIs which have the capability of dictating SMS functionality.
- EMS Control – identifies those IEIs which manage EMS Content IEIs.
- EMS Content – identifies those IEIs containing data of a unique media format.

It is permissible for certain IEs to be repeated within a short message, or within a concatenated message. There is no restriction on the repeatability of IEs in the EMS Content classification. The repeatability of SMS Control and EMS Control IEs is determined on an individual basis. See the IE table below for the repeatability of each IE.

In the event that IEs determined as not repeatable are duplicated, the last occurrence of the IE shall be used. In the event that two or more IEs occur which have mutually exclusive meanings (e.g. an 8bit port address and a 16bit port address), then the last occurring IE shall be used.

If the length of the User Data Header is such that there are too few or too many octets in the final Information Element then the whole User Data Header shall be ignored.

If any reserved values are received within the content of any Information Element then that part of the Information Element shall be ignored.

The support of any Information Element Identifier is optional unless otherwise stated.

The Information Element Identifier octet shall be coded as follows:

VALUE (hex)	MEANING	Classification	Repeatability
00	Concatenated short messages, 8-bit reference number	SMS Control	No
01	Special SMS Message Indication	SMS Control	Yes
02	Reserved	N/A	N/A
03	Value not used to avoid misinterpretation as <LF> character	N/A	N/A
04	Application port addressing scheme, 8 bit address	SMS Control	No
05	Application port addressing scheme, 16 bit address	SMS Control	No
06	SMSC Control Parameters	SMS Control	No
07	UDH Source Indicator	SMS Control	Yes
08	Concatenated short message, 16-bit reference number	SMS Control	No
09	Wireless Control Message Protocol	SMS Control	Note 3
0A	Text Formatting	EMS Control	Yes
0B	Predefined Sound	EMS Content	Yes
0C	User Defined Sound (iMelody max 128 bytes)	EMS Content	Yes
0D	Predefined Animation	EMS Content	Yes
0E	Large Animation (16*16 times 4 = 32*4 =128 bytes)	EMS Content	Yes
0F	Small Animation (8*8 times 4 = 8*4 =32 bytes)	EMS Content	Yes
10	Large Picture (32*32 = 128 bytes)	EMS Content	Yes
11	Small Picture (16*16 = 32 bytes)	EMS Content	Yes
12	Variable Picture	EMS Content	Yes
13	User prompt indicator	EMS Control	Yes
14	Extended Object	EMS Content	Yes
15	Reused Extended Object	EMS Control	Yes
16	Compression Control	EMS Control	No
17	Object Distribution Indicator	EMS Control	Yes
18	Standard WVG object	EMS Content	Yes
19	Character Size WVG object	EMS Content	Yes
1A	Extended Object Data Request Command	EMS Control	No
1B-1F	Reserved for future EMS features (see subclause 3.10)	N/A	N/A
20	RFC 5322 E-Mail Header	SMS Control	No
21	Hyperlink format element	SMS Control	Yes
22	Reply Address Element	SMS Control	No
23	Enhanced Voice Mail Information	SMS Control	No
24	National Language Single Shift	SMS Control	No
25	National Language Locking Shift	SMS Control	No
26 – 6F	Reserved for future use	N/A	N/A
70 – 7F	(U)SIM Toolkit Security Headers	SMS Control	Note 1
80 – 9F	SME to SME specific use	SMS Control	Note 2
A0 – BF	Reserved for future use	N/A	N/A
C0 – DF	SC specific use	SMS Control	Note 2
E0 – FF	Reserved for future use	N/A	N/A

Note 1: The functionality of these IEIs is defined in 3GPP TSG 31.115 [28], and therefore, the repeatability is not within the scope of this document and will not be determined here.

Note 2: The functionality of these IEIs is used in a proprietary fashion by different SMSC vendors, and therefore, are not within the scope of this technical specification.

Note 3: The functionality of these IEIs is defined by the WAP Forum and therefore the repeatability is not within the scope of this document and will not be determined here.

A receiving entity shall ignore (i.e. skip over and commence processing at the next information element) any information element where the IEI is Reserved or not supported. The receiving entity calculates the start of the next information element by looking at the length of the current information element and skipping that number of octets.

The SM itself may be coded as 7, 8 or 16 bit data.

If 7 bit data is used and the TP-UD-Header does not finish on a septet boundary then fill bits are inserted after the last Information Element Data octet up to the next septet boundary so that there is an integral number of septets for the entire TP-UD header. This is to ensure that the SM itself starts on an septet boundary so that an earlier Phase mobile shall be capable of displaying the SM itself although the TP-UD Header in the TP-UD field may not be understood.

It is optional to make the first character of the SM itself a Carriage Return character encoded according to the default 7 bit alphabet so that earlier Phase mobiles, which do not understand the TP-UD-Header, shall over-write the displayed TP-UD-Header with the SM itself.

If 16 bit (USC2) data is used then padding octets are not necessary. The SM itself shall start on an octet boundary.

If 8 bit data is used then padding is not necessary. An earlier Phase mobile shall be able to display the SM itself although the TP-UD header may not be understood.

It is also possible for mobiles not wishing to support the TP-UD header to check the value of the TP-UDHI bit in the SMS-Deliver PDU and the first octet of the TP-UD field and skip to the start of the SM and ignore the TP-UD header.

[TS 23.040, clause 9.2.3.24.1]:

This facility allows short messages to be concatenated to form a longer message.

In the case of uncompressed 8-bit data, the maximum length of the short message within the TP-UD field is 134 (140-6) octets.

In the case of uncompressed GSM 7 bit default alphabet data, the maximum length of the short message within the TP-UD field is 153 (160-7) characters. A character represented by an escape-sequence shall not be split in the middle.

In the case of 16 bit uncompressed USC2 data, the maximum length of the short message within the TP-UD field is 67 ((140-6)/2) characters. A UCS2 character shall not be split in the middle; if the length of the User Data Header is odd, the maximum length of the whole TP-UD field is 139 octets.

In the case of compressed GSM 7 bit default alphabet data, 8 bit data or UCS2 the maximum length of the compressed short message within the TP-UD field is 134 (140-6) octets including the Compression Header and Compression Footer, both or either of which may be present (see clause 3.9).

The maximum length of an uncompressed concatenated short message is 39015 (255*153) default alphabet characters, 34170 (255*134) octets or 17085 (255*67) UCS2 characters.

The maximum length of a compressed concatenated message is 34170 (255*134) octets including the Compression Header and Compression Footer (see clause 3.9 and figure 9.2.3.24.1(a) below).

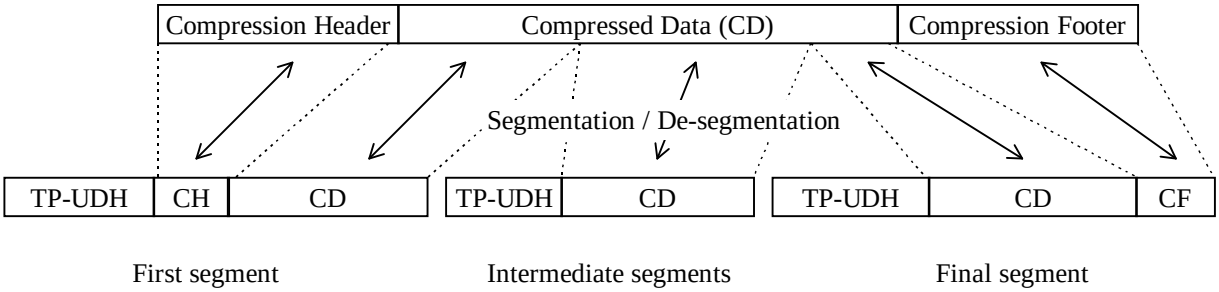

Figure 9.2.3.24.1 (a): Concatenation of a Compressed short message

The gNB-DU controlling a UE-associated logical F1-connection initiates the procedure by generating a UE The Information-Element-Data field contains information set by the application in the SMS-SUBMIT so that the receiving entity is able to re-assemble the short messages in the correct order. Each concatenated short message contains a reference number which together with the originating address and Service Centre address allows the receiving entity to discriminate between concatenated short messages sent from different originating SMEs and/or SCs. In a network which has multiple SCs, it is possible for different segments of a concatenated SM to be sent via different SCs and so it is recommended that the SC address should not be checked by the MS unless the application specifically requires such a check.

The TP elements in the SMS-SUBMIT PDU, apart from TP-MR, TP-SRR, TP-UDL and TP-UD, should remain unchanged for each SM which forms part of a concatenated SM, otherwise this may lead to irrational behaviour. TP-MR must be incremented for every segment of a concatenated message as defined in clause 9.2.3.6. A SC shall handle segments of a concatenated message like any other short message. The relation between segments of a concatenated message is made only at the originator, where the message is segmented, and at the recipient, where the message is

reassembled. SMS-COMMANDs identify messages by TP-MR and therefore apply to only one segment of a concatenated message. It is up to the originating SME to issue SMS-COMMANDs for all the required segments of a concatenated message.

The Information-Element-Data octets shall be coded as follows.

Octet 1 Concatenated short message reference number.

This octet shall contain a modulo 256 counter indicating the reference number for a particular concatenated short message. This reference number shall remain constant for every short message which makes up a particular concatenated short message.

Octet 2 Maximum number of short messages in the concatenated short message.

This octet shall contain a value in the range 0 to 255 indicating the total number of short messages within the concatenated short message. The value shall start at 1 and remain constant for every short message which makes up the concatenated short message. If the value is zero then the receiving entity shall ignore the whole Information Element.

Octet 3 Sequence number of the current short message.

This octet shall contain a value in the range 0 to 255 indicating the sequence number of a particular short message within the concatenated short message. The value shall start at 1 and increment by one for every short message sent within the concatenated short message. If the value is zero or the value is greater than the value in octet 2 then the receiving entity shall ignore the whole Information Element.

The IEI and associated IEI length and IEI data shall be present in every segment of the concatenated SM.

[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 [14];
- extract the payload encoded according to 3GPP TS 24.011 [8] 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 [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;

d) the In-Reply-To header which shall contain the Call-Id of the SIP MESSAGE request that was received in the received short message;

e) the Content-Type header shall contain "application/vnd.3gpp.sms"; and

f) 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 [14], clauses 5.3.2.3 and 5.3.2.4, and TS 23.040 [24], clauses 9.2.3.23, 9.2.3.24 and 9.2.3.24.1.

9.4.3 Test description

9.4.3.1 Pre-test conditions

System Simulator:

- 1 NR Cell connected to 5GC, default parameters.

UE:

- UE contains either ISIM and USIM applications or only USIM application on UICC.
- UE is configured to register for IMS after switch on.

Preamble:

- The UE is in test state 1N-A (TS 38.508-1) and registered to IMS.

9.4.3.2 Test procedure sequence

Table 9.4.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	SS sends a first segment of a concatenated SMS in the message-body of SIP_MESSAGE.	<--	SIP MESSAGE request		
2	Check: does UE respond with a 200 OK?	-->	200 OK	1	P
3	Check: when the payload is extracted, does the UE respond with a delivery report included in the message-body of MESSAGE?	-->	SIP MESSAGE request	1	P
4	SS responds with a 202 ACCEPTED.	<--	202 ACCEPTED		
5	SS sends a second segment of a concatenated SMS in the message-body of SIP_MESSAGE.	<--	SIP MESSAGE request		
6	Check: does UE respond with a 200 OK?	-->	200 OK	2	P
7	Check: when the payload is extracted, does the UE respond with a delivery report included in the message-body of MESSAGE?	-->	SIP MESSAGE request	2	P
8	SS responds with a 202 ACCEPTED.	<--	202 ACCEPTED		
9	SS sends a final segment of a concatenated SMS in the message-body of SIP_MESSAGE.	<--	SIP MESSAGE request		
10	Check: does UE respond with a 200 OK?	-->	200 OK	3	P
11	Check: when the payload is extracted, does the UE respond with a delivery report included in the message-body of MESSAGE?	-->	SIP MESSAGE request	3	P
12	SS responds with a 202 ACCEPTED.	<--	202 ACCEPTED		

9.4.3.3 Specific message contents

Table 9.4.3.3-1: MESSAGE for MT SMS (step 1, table 9.4.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in annex A.7.1				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Message-body		- TP-RP='0'B (TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER) - TP-MMS='0'B (More messages are waiting for the MS in this SC) - TP-UDHI='1'B (The beginning of the TP UD field contains a Header in addition to the short message.) - TP-PID='00000000'B - TP-UD - Length of User Data Header (UDHL)=5 - Information Element Identifier (IEI)=0x00 (Concatenated short messages, 8-bit reference number) - Length of Information Element (IEIDL)=3 - Concatenated short message reference number=any allowed value - Maximum number of short messages in the concatenated short message=3 - Sequence number of the current short message=1		TS 24.011 [25] TS 23.040 [24]

Table 9.4.3.3-2: 200 OK for other requests than REGISTER or SUBSCRIBE (step 2/6/10, table 9.4.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.3.1, Condition A22

Table 9.4.3.3-3: MESSAGE for delivery report (step 3/7/11, table 9.4.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.7.2

Table 9.4.3.3-4: 202 ACCEPTED (step 4/8, table 9.4.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.3.3

Table 9.4.3.3-5: MESSAGE for MT SMS (step 5, table 9.4.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in annex A.7.1				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Message-body		- TP-RP='0'B (TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER) - TP-MMS='0'B (More messages are waiting for the MS in this SC) - TP-UDHI='1'B (The beginning of the TP UD field contains a Header in addition to the short message.) - TP-PID='00000000'B - TP-UD - Length of User Data Header (UDHL)=5 - Information Element Identifier (IEI)=0x00 (Concatenated short messages, 8-bit reference number) - Length of Information Element (IEIDL)=3 - Concatenated short message reference number=The same value sent in the step1 - Maximum number of short messages in the concatenated short message=3 - Sequence number of the current short message=2		TS 24.011 [25] TS 23.040 [24]

Table 9.4.3.3-6: MESSAGE for MT SMS (step 9, table 9.4.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in annex A.7.1				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Message-body		- TP-RP='0'B (TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER) - TP-MMS='0'B (More messages are waiting for the MS in this SC) - TP-UDHI='1'B (The beginning of the TP UD field contains a Header in addition to the short message.) - TP-PID='00000000'B - TP-UD - Length of User Data Header (UDHL)=5 - Information Element Identifier (IEI)=0x00 (Concatenated short messages, 8-bit reference number) - Length of Information Element (IEIDL)=3 - Concatenated short message reference number=The same value sent in the step1 - Maximum number of short messages in the concatenated short message=3 - Sequence number of the current short message=3		TS 24.011 [25] TS 23.040 [24]

9.5 Mobile Originating SMS / RP-ERROR / 5GS

9.5.1 Test Purpose (TP)

(1)

```
with { UE being registered to IMS }
ensure that {
  when { UE is made to send an SMS over IP }
    then { UE sends a SIP MESSAGE request containing a short message }
    }
```

(2)

```
with { UE having sent a SIP MESSAGE request containing a short message }
ensure that {
  when { UE receives a 202 Accepted response, followed by a SIP MESSAGE request containing an RP-
ERROR message }
    then { UE sends a 200 OK response }
    }
```

9.5.2 Conformance Requirements

[TS 24.341, clause 5.3.1.1]:

In addition to the procedures specified in subclause 5.3.1, the SM-over-IP sender shall support the procedures specified in 3GPP TS 24.229 [10] appropriate to the functional entity in which the SM-over-IP sender is implemented. The SM-over-IP sender shall build and populate RP-DATA message, containing all the information that a mobile station submitting an SM according to 3GPP TS 24.011 [8] would place, for successful delivery. The SM-over-IP sender shall parse and interpret RP- DATA, RP-ACK and RP-ERROR messages, containing all the information that a mobile station receiving an SM according to 3GPP TS 24.011 [8] would see, in a SM submission or status report.

NOTE 1: If the SM-over-IP sender uses SMR entity timers as specified in 3GPP TS 24.011 [8], then TR1M is set to a value greater than timer F (see 3GPP TS 24.229 [10]).

NOTE 2: If the SM-over-IP sender expects to receive a SM submit report will include the "+g.3gpp.smsip" parameter in the Contact header field when sending a REGISTER request.

[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 an ISIM is present, then the PSI of the SC is obtained from the $EF_{PSISMSC}$ in DF_TELECOM as per 3GPP TS 31.103 [18];

- if an ISIM is not present, then the PSI of the SC is obtained from the $EF_{PSISMSC}$ in DF_TELECOM as per 3GPP TS 31.102 [19]; or

- if the PSI of the SC is not available in $EF_{PSISMSC}$ in DF_TELECOM, 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 PSI of 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;

d) the In-Reply-To header which shall contain the Call-Id of the SIP MESSAGE request that was received in the received short message;

e) the Content-Type header shall contain "application/vnd.3gpp.sms"; and

f) 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.

[TS 24.011 clause 8.2.5.4]:

This element is a variable length element always included in the RP-ERROR message, conveying a negative result of a RP-DATA message transfer attempt or RP-SMMA notification attempt. The element contains a cause value and optionally a diagnostic field giving further details of the error cause.

The coding of the cause value is given in table 8.4/3GPP TS 24.011. The mapping between error causes in 3GPP TS 24.011 and 3GPP TS 29.002 (MAP) is specified in 3GPP TS 23.040. Parameters included in the return error from MAP (e.g. System Failure) are mapped directly into the diagnostic field.

8 7 6 5 4 3 2 1		
0	1 0 0 0 0 1 0 RP-Cause IEI	1 octet
Length indicator		1 octet
0 ext	Cause value Cause value	1 octet
Diagnostic field		1 octet *

Figure 8.8/3GPP TS 24.011: RP-Cause element layout

Table 8.4/3GPP TS 24.011 (part 1): Cause values that may be contained in an RP-ERROR message in a mobile originating SM-transfer attempt

Cause value	Cause number	Cause
7 6 5 4 3 2 1	#	
0 0 0 0 0 0 1	1	Unassigned (unallocated) number
0 0 0 1 0 0 0	8	Operator determined barring
0 0 0 1 0 1 0	10	Call barred
0 0 0 1 0 1 1	11	Reserved
0 0 1 0 1 0 1	21	Short message transfer rejected
0 0 1 1 0 1 1	27	Destination out of order
0 0 1 1 1 0 0	28	Unidentified subscriber
0 0 1 1 1 0 1	29	Facility rejected
0 0 1 1 1 1 0	30	Unknown subscriber
0 1 0 0 1 1 0	38	Network out of order
0 1 0 1 0 0 1	41	Temporary failure
0 1 0 1 0 1 0	42	Congestion
0 1 0 1 1 1 1	47	Resources unavailable, unspecified
0 1 1 0 0 1 0	50	Requested facility not subscribed
1 0 0 0 1 0 1	69	Requested facility not implemented
1 0 1 0 0 0 1	81	Invalid short message transfer reference value
1 0 1 1 1 1 1	95	Semantically incorrect message
1 1 0 0 0 0 0	96	Invalid mandatory information
1 1 0 0 0 0 1	97	Message type non-existent or not implemented
1 1 0 0 0 1 0	98	Message not compatible with short message protocol state
1 1 0 0 0 1 1	99	Information element non-existent or not implemented
1 1 0 1 1 1 1	111	Protocol error, unspecified
1 1 1 1 1 1 1	127	Interworking, unspecified
Note: All other cause values shall be treated as cause number 41, "Temporary Failure"		

Reference(s)

3GPP TS 24.341[14], clauses 5.3.1.1, 5.3.1.2, 5.3.1.3 and 5.3.2.4, and TS 24.011 [25], clause 8.2.5.4.

9.5.3 Test description

9.5.3.1 Pre-test conditions

System Simulator:

- 1 NR Cell connected to 5GC, default parameters.

UE:

- UE contains either ISIM and USIM applications or only USIM application on UICC.
- UE is configured to register for IMS after switch on.
- SMS over IP is enabled.

Preamble:

- The UE is in test state 1N-A (TS 38.508-1 [21]) and registered to IMS.

9.5.3.2 Test procedure sequence

Table 9.5.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	UE is made to send an SMS over IP.				
2	Check: does the UE send a SIP MESSAGE request including a vnd.3gpp.sms payload that contains a short message?	-->	SIP MESSAGE request	1	P
3	SS responds with 202 Accepted.	<--	202 ACCEPTED		
4	SS sends a SIP MESSAGE request including a vnd.3gpp.sms payload and RP-ERROR message.	<--	SIP MESSAGE request		
5	Check: does the UE respond with 200 OK?	-->	200 OK	2	P

9.5.3.3 Specific message contents

Table 9.5.3.3-1: Message for MO SMS (step 2, table 9.5.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in annex A.7.3, Condition A2, A5

Table 9.5.3.3-2: 202 ACCEPTED (step 3, table 9.5.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.3.3

Table 9.5.3.3-3: Short message submission report for MO SMS (step 4, table 9.5.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in annex A.7.4				
Header/param	**Cond**	**Value/remark**	**Rel**	**Reference**
Message-body		RP-ERROR message with RP-Cause Data: Length: 2, Length indicator = 1 Extension: not extended Cause value: 38 (Network out of order)		TS 24.011 [25] TS 23.040 [24]

Table 9.5.3.3-4: 200 OK for other requests than REGISTER or SUBSCRIBE (step 5, table 9.5.3.2-1)

Derivation Path: TS 34.229-1 [2], Table in subclause A.3.1, Condition A5, A22

10

10.1 Emergency Call with emergency registration / Success / Location information available / 5GS

10.1.1 Test Purpose (TP)

(1)

```
with { UE being registered to IMS }
ensure that {
  when { UE is being made to initiate an emergency call }
    then { UE sends a correctly composed initial REGISTER request for IMS emergency registration }
```

(2)

```
with { UE having sent an unprotected REGISTER request }
ensure that {
  when { UE receiving a valid 401 (Unauthorized) response for the initial REGISTER request sent }
    then { UE correctly authenticates itself by sending another REGISTER request with a correctly
composed Authorization header using the AKAv1-MD5 algorithm }
    }
```

(3)

```
with { UE having sent unprotected and then protected REGISTER request }
ensure that {
  when { UE receiving a valid 200 OK response for the REGISTER sent for authentication }
    then { UE sends a correctly composed INVITE request }
    }
```

(4)

```
with { UE having sent INVITE }
ensure that {
  when { UE receiving 100 Trying, followed by 180 Ringing, followed by 200 OK }
    then { UE sends ACK }
      }
```

(5)

```
with { Emergency call being established }
ensure that {
  when { UE receives BYE  }
    then { UE sends a 200 OK response }
    }
```

10.1.2 Conformance Requirements

[TS 24.229 clause 4.7.5]:

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); and

...

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 [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.

NOTE 1: For CS systems based on 3GPP TS 24.008 [8], clause B.5 applies.

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 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 and 5.1.3 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 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 WLAN access node, which is relevant for routeing the IMS emergency call;

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.

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], and include a Content-Disposition header field with a disposition type "render" value and a "handling" header field parameter with an "optional" value, as described in RFC 3261 [26];

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];

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; and

10) if support of the current location discovery during an emergency call is allowed in the IP-CAN specific annex and the UE supports the current location discovery during an emergency call, the UE shall include a Recv-Info header field as described in RFC 6086 [25], indicating the g.3gpp.current-location-discovery info package name and shall include an Accept header field indicating the "application/vnd.3gpp.current-location-discovery+xml" MIME type.

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 an 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 [8J]. 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 2: In this respect an equivalent HPLMN, as defined in 3GPP TS 23.122 [4C] 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 [2] and if the SC UE has an IMEI, then the SC UE shall include the sip.instance media feature tag as specified in IETF RFC 5626 [22] with value based on the IMEI as defined in 3GPP TS 23.003 [12] in the Contact header field of the SIP INVITE request according to IETF RFC 3840 [53].

[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 RFC 7254 [79]). The format of the instance-id shall take the form "urn:gsma:imei:<imeival>" where by the imeival shall contain the IMEI encoded as defined in RFC 7254 [79]. The optional <sw-version-param> and <imei-version-param> parameters shall not be included in the instance-id. RFC 7255 [104] specifies additional considerations for using the IMEI as an instance-id. An example of such an instance-id is as follows:

EXAMPLE: urn:gsma:imei:90420156-025763-0

If no IMEI is available, the instance-id shall take the form of a string representation of a UUID as a URN as defined in IETF RFC 4122 [80]. An example of such an instance-id is as follows:

EXAMPLE: urn:uuid:f81d4fae-7dec-11d0-a765-00a0c91e6bf6

For more information on the instance-id and when it is used, see 3GPP TS 24.229 [81].

Reference(s)

3GPP TS 24.229 [7], clauses 5.1.6.1, 5.1.6.2, 5.1.6.8.3 and Annex L2.2.6, TS 24.237 [26] clause 7.2 and TS 23.003 [27] clause 13.8 (release 9).

10.1.3 Test description

10.1.3.1 Pre-test conditions

System Simulator:

- 1 NR Cell connected to 5GC, default parameters.

UE:

- UE contains either ISIM and USIM applications or only USIM application on UICC.
- UE is configured to register for IMS after switch on.

Preamble:

- The UE is in test state 1N-A (TS 38.508-1) and registered to IMS.

10.1.3.2 Test procedure sequence

Table 10.1.3.2-1: Main Behaviour

St	Procedure	Message Sequence		TP	Verdict
		U - S	Message		
1	UE is made to make an emergency call				
2	Step 1 of annex A.3 (emergency registration) Check: Does the UE send a correctly composed initial REGISTER request for IMS emergency registration?	-->	REGISTER	1	P
3	Step 2 of annex A.3 (emergency registration)	<--	401 Unauthorized		
4	Step 3 of annex A.3 (emergency registration) Check: Does the UE correctly authenticate itself by sending another REGISTER request with a correctly composed Authorization header using the AKAv1-MD5 algorithm?	-->	REGISTER	2	P
5	Step 4 of annex A.3 (emergency registration)	<--	200 OK		
6	Step 1 of annex A.6 (emergency call) Check: Does the UE send a correctly composed INVITE request?	-->	INVITE	3	P
7	Step 2 of annex A.6 (emergency call)	<--	100 Trying		
8	Step 3 of annex A.6 (emergency call)	<--	180 Ringing		
9	Step 4 of annex A.6 (emergency call)	<--	200 OK		
10	Step 5 of annex A.6 (emergency call) Check: Does the UE send ACK?	-->	ACK	4	P
11	Step 1 of annex A.8 (MT Release of Voice Call)	<--	BYE		
12	Step 2 of annex A.8 (MT Release of Voice Call) Check: Does the UE send 200 OK for the BYE request and ends the call?	-->	200 OK	5	P

10.1.3.3 Specific message contents

None as fully described in annex A.3, A.6 and A.8.

Annex A (normative): Generic Test Procedures

A.1 Introduction

This annex specifies general procedures for IMS usages as well as application specific procedures, e.g. for a MTSI client.

A.2 IMS Registration / 5GS

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	→		REGISTER	The 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	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.
-			EXCEPTION: In parallel to the events described in steps 5-8, the steps specified in Annex C.5 of TS 34.229-1 [2] on PUBLISH may happen.	The PUBLISH request uses conditions A1 and A5.
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.

Specific Message Contents

REGISTER (Step 1)

Use the default message "REGISTER" in Annex A.1.1 of TS 34.229-1 [2] applying conditions A1 and A32.

401 Unauthorized (Step 2)

Use the default message "401 Unauthorized for REGISTER" in Annex A.1.2 of TS 34.229-1 [2] applying condition A1.

REGISTER (Step 3)

Use the default message "REGISTER" in Annex A.1.1 of TS 34.229-1 [2] applying conditions A2 and A32.

200 OK (Step 4)

Use the default message "200 OK for REGISTER" in Annex A.1.3 of TS 34.229-1 [2] applying condition A2.

SUBSCRIBE (Step 5)

Use the default message "SUBSCRIBE for reg-event package" in Annex A.1.4 of TS 34.229-1 [2] applying conditions A1 and A7.

200 OK (Step 6)

Use the default message "200 OK for SUBSCRIBE" in Annex A.1.4 of TS 34.229-1 [2] applying condition A1.

NOTIFY (Step 7)

Use the default message "NOTIFY for reg-event package" in Annex A.1.6 of TS 34.229-1 [2] applying condition A1.

200 OK (Step 8)

Use the default message "200 OK for requests other than REGISTER or SUBSCRIBE" in Annex A.3.1 of TS 34.229-1 [2] applying conditions A5, A8, and A22.

A.3 IMS Emergency Registration / 5GS

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.

Specific Message Contents:

REGISTER (Step 1)

Use the default message “REGISTER” in Annex A.1.1 of TS 34.229-1 [2] with conditions A1 and A7.

401 Unauthorized (Step 2)

Use the default message “401 Unauthorized for REGISTER” in Annex A.1.2 of TS 34.229-1 [2] with condition A1.

REGISTER (Step 3)

Use the default message “REGISTER” in Annex A.1.1 of TS 34.229-1 [2] with conditions A2, A7, and A32.

200 OK for REGISTER (Step 4)

Use the default message “200 OK for REGISTER” in Annex A.1.3 of TS 34.229-1 [2] with condition A3.

A.4 MTSI MO Voice Call / 5GS

A.4.1 MTSI MO Voice Call / with preconditions / 5GS

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	←		183 Session Progress	SS sends an SDP answer.
4	→		PRACK	UE acknowledges reception of 183 Session Progress.
5	←		200 OK	SS responds to PRACK.
6	→		UPDATE	UE sends a second SDP offer in an UPDATE request.
7	←		200 OK	SS responds to UPDATE.
8	←		180 Ringing	SS sends 180 Ringing reliably.
9	→		PRACK	UE acknowledges reception of 180 Ringing.
10	←		200 OK	SS responds to PRACK.
11	←		200 OK	SS responds to INVITE.
12	→		ACK	UE acknowledges.
NOTE: The test procedure including NR/5GC signalling is specified in TS 38.508 [21] subclause 4.9.15.				

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MO Call Setup" in Annex A.2.1 of TS 34.229-1 [2] applying conditions A1, A3, A4 and A28, and 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) [Note 2] *b=RR:* (bandwidth-value) [Note 2] **Attributes for media:** *a=rtpmap:* (payload type) *EVS/16000* [Note 3, 9, 10] *a=fmtp:* (format) *br=5.9-13.2; bw=nb-swb; max-red=* (att-field) [Note 4, 5, 10] *a=rtpmap:* (payload type) *EVS/16000* [Note 3, 9, 10] *a=fmtp:* (format) *br=5.9-24.4; bw=nb-swb; max-red=* (att-field) [Note 4, 5, 10] *a=rtpmap:* (payload type) *EVS/16000* [Note 3, 9, 10] *a=fmtp:* (format) *br=13.2; bw=swb; max-red=* (att-field) [Note 4, 5, 10] *a=rtpmap:* (payload type) *EVS/16000* [Note 3, 9, 10] *a=fmtp:* (format) *br=9.6-13.2; bw=swb; max-red=* (att-field) [Note 4, 5, 10] *a=rtpmap:* (payload type) *EVS/16000* [Note 3, 9, 10] *a=fmtp:* (format) *br=9.6-24.4; bw=swb; max-red=* (att-field) [Note 4, 5, 10] *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 3, 9] *a=fmtp:* (format) *mode-change-capability=2; max-red=* (att-field) [Note 4, 6] *a=rtpmap:* (payload type) *telephone-event/16000* *a=fmtp:* (format) *a=rtpmap:* (payload type) *AMR/8000* [Note 3, 9] *a=fmtp:* (format) *mode-change-capability=2; max-red=* (att-field) [Note 4, 6] *a=rtpmap:* (payload type) *telephone-event/8000* *a=fmtp:* (format) *a=ecn-capable-rtp: leap ect=0* [Note 7] *a=rtcp-fb:* nack ecn* [Note 7] *a=rtcp-xr:ecn-sum* [Note 7] *a=rtcp-rsize* [Note 7] *a=ptime:20* *a=maxptime:240* **Attributes for media security mechanism:** *a=3ge2ae: requested* [Note 8] *a=crypto:1 AES_CM_128_HMAC_SHA1_80inline:WVNfX19zZW1jdGwgKCkgewkyMjA7fQp9 CnVubGVz|2^20|* *1:4FEC_ORDER=FEC_SRTP"* [Note 8] **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 RR value shall be greater than 0. The RS value can be any value. Note 3: The channel number shall be "/1" or omitted. Note 4: The max-red values from 0 to 220 are allowed. Note 5: The parameters dtx, dtx-recv and evs-mode-switch shall not be present. Note 6: The parameters mode-set, mode-change-period, mode-change-neighbor, crc, robust-sorting and interleaving shall not be included. Note 7: Attributes for ECN Capability may be present if the UE supports Explicit Congestion Notification. Note 8: Attributes for media plane security are present if the use of end-to-access-edge security is supported by UE.

	Note 9: The ordering of payload types shall be as listed, i.e., EVS before AMR-WB before AMR. Note 10: The EVS payload type shall carry at least one of the five EVS configurations

100 Trying (Step 2)

Use the default message "100 Trying for INVITE" in Annex A.2.2 of TS 34.229-1 [2] applying condition A1.

183 Session Progress (Step 3)

Use the default message "183 Session Progress for INVITE" in Annex A.2.3 of TS 34.229-1 [2] applying condition A1, and with the following exceptions:

Header/param	Value/Remark
Require 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=-* *c=IN* (addrtype) (connection-address for SS) *b=AS:65* **Time description:** *t=0 0* **Media description:** *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1, 2] *b=AS:65* *b=RS:* (bandwidth-value) [Note 3] *b=RR:* (bandwidth-value) [Note 3] **Attributes for media:** *a=rtpmap:* (payload type) *EVS/16000/1* [Note 1, 8] *a=fmtp:* (format) *br=13.2; bw=swb; mode-set=0,1,2; max-red=220* [Note 8] *a=rtpmap:* (payload type) *EVS/16000/1* [Note 1, 9] *a=fmtp:* (format) *br=5.9-13.2; bw=nb-swb; mode-set=0,1,2, max-red=220* [Note 9] *a=ecn-capable-rtp: leap ect=0* [Note 6] *a=rtcp-fb:* nack ecn* [Note 6] *a=rtcp-xr:ecn-sum* [Note 6] *a=ptime:20* *a=maxptime:240* **Attributes for media security mechanism:** *a=3ge2ae: requested* [Note 7] *a=crypto:1 AES_CM_128_HMAC_SHA1_80inline:PS1uQCVeeCFCanVmcjkpPywjNWhcYD0mX XtxaVBR|2^20|1:4* [Note 7] **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 values for fmt, payload type and format are copied from step 1. Note 2: Transport port is the port number of the SS (see RFC 3264 clause 6). Note 3: The bandwidth-value is copied from step 1. Note 4: All present br, br-send and br-recv parameter=value pairs are copied from step 1. Note 5: bw, bw-send and bw-recv parameter are copied from bw at step 1. Note 6: Attributes for ECN Capability are present if the UE supports Explicit Congestion Notification. Note 7: Attributes for media plane security are present if the use of end-to-access-edge security is supported by UE. Note 8: This EVS configuration is sent if UE sent it as the first of its EVS configurations in INVITE. Note 9: This EVS configuration is sent if UE did not send "br=13.2; bw=swb" as the first of its EVS configurations in INVITE.

PRACK (Step 4)

Use the default message "PRACK" in Annex A.2.4 of TS 34.229-1 [2] applying conditions A1 and A7.

200 OK for PRACK (Step 5)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 of TS 34.229-1 [2] applying conditions A10 and A22.

UPDATE (Step 6)

Use the default message "UPDATE" in Annex A.2.5 of TS 34.229-1 [2] applying conditions A1 and A6, and with the following exceptions:

Header/param	Value/Remark
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) [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) *EVS/16000* [Note 3] [Note 5] *a=fmtp:* (format) [Note 3] [Note 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* or *a=des:qos mandatory remote sendrecv* Note 1: At least one "c=" field shall be present. Note 2: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one Note 3: The value for fmt, payload type and format is not checked Note 4: Parameters for the codec are not checked Note 5: The channel number shall be "/1" or omitted.

200 OK for UPDATE (Step 7)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 of TS 34.229-1 [2] applying conditions A1, A10 and A22, and with the following exceptions:

Header/param	Value/remark
Require option-tag	*precondition*
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 and modified as follows: - IP address on "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; - "o=" line identical to previous SDP sent by SS except that sess-version is incremented; - Attributes for preconditions: *a=curr:qos remote sendrecv*

180 Ringing (Step 8)

Use the default message "180 Ringing for INVITE" in Annex A.2.6 of TS 34.229-1 [2] applying conditions A1 and A3.

PRACK (Step 9)

Use the default message "PRACK" in Annex A.2.4 of TS 34.229-1 [2] applying conditions A1 and A7.

200 OK for PRACK (Step 10)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 of TS 34.229-1 [2] applying condition A10.

200 OK for INVITE (Step 11)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 of TS 34.229-1 [2] applying conditions A1, A10, and A19.

ACK (Step 12)

Use the default message "ACK" in Annex A.2.6 of TS 34.229-1 [2] applying conditions A1 and A3.

A.4.2 MTSI MO Voice Call / without preconditions / 5GS

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	←		183 Session Progress	SS sends an SDP answer.
4	→		PRACK	UE acknowledges reception of 183 Session Progress.
5	←		200 OK	SS responds to PRACK.
6	←		180 Ringing	SS sends 180 Ringing.
7	←		200 OK	SS responds to INVITE.
8	→		ACK	UE acknowledges.
NOTE: The test procedure including NR/5GC signalling is specified in TS 38.508 [21] subclause 4.9.15.				

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MO Call" in Annex A.2.1 of TS 34.229-1 [2] applying conditions A1, A3, A4 and A28, and 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] *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) [Note 2] *b=RR:* (bandwidth-value) [Note 2] **Attributes for media:** *a=rtpmap:* (payload type) *EVS/16000* [Note 3, 9, 10] *a=fmtp:* (format) *br=5.9-13.2; bw=nb-swb; max-red*= (att-field) [Note 4, 5, 10] *a=rtpmap:* (payload type) *EVS/16000* [Note 3, 9, 10] *a=fmtp:* (format) *br=5.9-24.4; bw=nb-swb; max-red*= (att-field) [Note 4, 5, 10] *a=rtpmap:* (payload type) *EVS/16000* [Note 3, 9, 10] *a=fmtp:* (format) *br=13.2; bw=swb; max-red*= (att-field) [Note 4, 5, 10] *a=rtpmap:* (payload type) *EVS/16000* [Note 3, 9, 10] *a=fmtp:* (format) *br=9.6-13.2; bw=swb; max-red*= (att-field) [Note 4, 5, 10] *a=rtpmap:* (payload type) *EVS/16000* [Note 3, 9, 10] *a=fmtp:* (format) *br=9.6-24.4; bw=swb; max-red*= (att-field) [Note 4, 5, 10] *a=rtpmap:* (payload type) *AMR-WB/16000* [Note 3, 9] *a=fmtp:* (format) *mode-change-capability=2; max-red*= (att-field) [Note 4, 6] *a=rtpmap:* (payload type) *telephone-event/16000* *a=fmtp:* (format) *a=rtpmap:* (payload type) *AMR/8000* [Note 3, 9] *a=fmtp:* (format) *mode-change-capability=2; max-red*= (att-field) [Note 4, 6] *a=rtpmap:* (payload type) *telephone-event/8000* *a=fmtp:* (format) *a=ecn-capable-rtp: leap ect=0* [Note 7] *a=rtcp-fb:* nack ecn* [Note 7] *a=rtcp-xr:ecn-sum* [Note 7] *a=rtcp-rsize* [Note 7] *a=ptime:20* *a=maxptime:240* **Attributes for media security mechanism:** *a=3ge2ae: requested* [Note 8] *a=crypto:1 AES_CM_128_HMAC_SHA1_80inline:WVNfX19zZW1jdGwgKCkgewkyMjA7fQp9 CnVubGVz|2^20|* *1:4FEC_ORDER=FEC_SRTP"* [Note 8] Note 1: At least one "c=" field shall be present. Note 2: The RR value shall be greater than 0. The RS value can be any value. Note 3: The channel number shall be "/1" or omitted. Note 4: The max-red values from 0 to 220 are allowed. Note 5: The parameters dtx, dtx-recv and evs-mode-switch shall not be present. Note 6: The parameters mode-set, mode-change-period, mode-change-neighbor, crc, robust-sorting and interleaving shall not be included. Note 7: Attributes for ECN Capability may be present if the UE supports Explicit Congestion Notification. Note 8: Attributes for media plane security are present if the use of end-to-access-edge security is supported by UE. Note 9: The ordering of payload types shall be as listed, i.e., EVS before AMR-WB before AMR. Note 10: The EVS payload type shall carry at least one of the five EVS configurations

100 Trying (Step 2)

Use the default message "100 Trying for INVITE" in Annex A.2.2 of TS 34.229-1 [2] applying condition A1.

183 Session Progress (Step 3)

Use the default message "183 Session Progress" in Annex A.2.3 of TS 34.229-1 [2] applying condition A1, and with 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=-* *c=IN* (addrtype) (connection-address for SS) *b=AS:65* **Time description:** *t=0 0* **Media description:** *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1, 2] *b=AS:65* *b=RS:* (bandwidth-value) [Note 3] *b=RR:* (bandwidth-value) [Note 3] **Attributes for media:** *a=rtpmap:* (payload type) *EVS/16000/1* [Note 1, 8] *a=fmtp:* (format) *br=13.2; bw=swb; mode-set=0,1,2; max-red=220* [Note 8] *a=rtpmap:* (payload type) *EVS/16000/1* [Note 1, 9] *a=fmtp:* (format) *br=5.9-13.2; bw=nb-swb; mode-set=0,1,2, max-red=220* [Note 9] *a=ecn-capable-rtp: leap ect=0* [Note 6] *a=rtcp-fb:* nack ecn* [Note 6] *a=rtcp-xr:ecn-sum* [Note 6] *a=ptime:20* *a=maxptime:240* **Attributes for media security mechanism:** *a=3ge2ae: requested* [Note 7] *a=crypto:1 AES_CM_128_HMAC_SHA1_80inline:PS1uQCVeeCFCanVmcjkpPywjNWhcYD0 mXXtxaVBR|2^20|1:4* [Note 7] Note 1: The values for fmt, payload type and format are copied from step 1. Note 2: Transport port is the port number of the SS (see RFC 3264 clause 6). Note 3: The bandwidth-value is copied from step 1. Note 4: All present br, br-send and br-recv parameter=value pairs are copied from step 1. Note 5: bw, bw-send and bw-recv parameter are copied from bw at step 1. Note 6: Attributes for ECN Capability are present if the UE supports Explicit Congestion Notification. Note 7: Attributes for media plane security are present if the use of end-to-access-edge security is supported by UE. Note 8: This EVS configuration is sent if UE sent it as the first of its EVS configurations in INVITE. Note 9: This EVS configuration is sent if UE did not send "br=13.2; bw=swb" as the first of its EVS configurations in INVITE.

PRACK (Step 4)

Use the default message "PRACK" in Annex A.2.4 of TS 34.229-1 [2] applying conditions A1 and A7.

200 OK for PRACK (Step 5)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 of TS 34.229-1 [2] applying conditions A10 and A22.

180 Ringing (Step 6)

Use the default message "180 Ringing for INVITE" in Annex A.2.6 of TS 34.229-1 [2] applying conditions A1 and A14.

200 OK for INVITE (Step 7)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 of TS 34.229-1 [2] applying conditions A1, A10, and A19.

ACK (Step 8)

Use the default message "ACK" in Annex A.2.6 of TS 34.229-1 [2] applying conditions A1 and A3.

A.5 MTSI MT Voice Call / 5GS

A.5.1 MTSI MT Voice Call / with preconditions / 5GS

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with the first SDP offer.
2	→		100 Trying	Optional step: UE may send a 100 Trying provisional response.
3	→		183 Session Progress	UE sends 183 Session Progress response reliably, including an SDP answer.
4	←		PRACK	SS acknowledges reception of 183 Session Progress.
5	→		200 OK	UE responds to PRACK.
6	←		UPDATE	SS sends a second SDP offer
7	→		200 OK	UE responds to UPDATE, including an SDP answer.
8	→		180 Ringing	UE sends 180 Ringing.
9	←		PRACK	Conditional step: if UE sent 180 Ringing reliably, SS acknowledges reception of 180 Ringing
10	→		200 OK	Conditional step: if UE sent 180 Ringing reliably, UE responds to PRACK.
11	→		200 OK	UE responds to INVITE.
12	←		ACK	SS acknowledges.
NOTE: The test procedure including NR/5GC signalling is specified in TS 38.508 [21] subclause 4.9.16.				

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MT Call" in Annex A.2.9 of TS 34.229-1 [2] applying conditions A1, A3, and A4, and 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=-* *c=IN* (addrtype) (connection-address for SS) *b=AS:65* Time description: *t=0 0* Media description: *m=audio* (transport port) *RTP/AVP 96 97 98 99 100* *b=AS:65* *b=RS:0* *b=RR:2000* Attributes for media: *a=rtpmap: 96 EVS/16000* *a=fmtp: 96 br=13.2; bw=swb; max-red=220* *a=rtpmap:97 AMR-WB/16000/1* *a=fmtp:97 mode-change-capability=2; max-red=220* *a=rtpmap: 98 telephone-event/16000* *a=fmtp: 98 0-15* *a=rtpmap:99 AMR/8000/1* *a=fmtp:99 mode-change-capability=2; max-red=220* *a=rtpmap: 100 telephone-event/8000* *a=fmtp: 100 0-15* *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*

100 Trying (Step 2)

Use the default message "100 Trying for INVITE" in Annex A.2.2 of TS 34.229-1 [2] applying condition A2.

183 Session Progress (Step 3)

Use the default message "183 Session Progress" in Annex A.2.3 of TS 34.229-1 [2] applying condition A2, and 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=*(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) *EVS/16000* [Note 2] *a=fmtp:*(format) *br=13.2; bw=swb; max-red=220* 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* Note 1: At least one "c=" field shall be present. Note 2: The value for fmt, payload type and format is not checked

PRACK (Step 4)

Use the default message "PRACK" in Annex A.2.4 of TS 34.229-1 [2] applying condition A3.

200 OK (Step 5)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 of TS 34.229-1 [2] applying conditions A5, A8, A11, and A22.

UPDATE (step 6)

Use the default message "UPDATE" in Annex A.2.5 of TS 34.229-1 [2] applying condition A3, and with the following exceptions:

Header/param	Value/remark
Require option-tag	*precondition*
Message-body	The following SDP types and values. Session description: *v=0* *o=- 1111111111 1111111112 IN* (addrtype) (unicast-address for SS) *s=-* *c=IN* (addrtype) (connection-address for SS) *b=AS:65* Time description: *t=0 0* Media description: *m=audio* (transport port) *RTP/AVP 96* *b=AS:65* *b=RS:0* *b=RR:2000* Attributes for media: *a=rtpmap:96 EVS/16000/1* *a=fmtp:96 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 7)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 of TS 34.229-1 [2] applying conditions A2, A11, and A22, and with the following exceptions:

Header/param	Value/remark
Require option-tag	*precondition*
Content-Type media-type	*application/sdp*
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body 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) [Note 4] *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) *EVS/16000* [Note 2] *a=fmtp:*(format) [Note 2, 3] 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 Note 4: "o=" line identical to previous SDP sent by UE except that sess-version is incremented by one.

180 Ringing (Step 8)

Use the default message "180 Ringing for INVITE" in Annex A.2.6 of TS 34.229-1 [2] applying conditions A2 and A14, and with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header not present
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body 0
Message-body	Not present

PRACK (Step 9)

Use the default message "PRACK" in Annex A.2.4 of TS 34.229-1 [2] applying condition A3.

200 OK (Step 10)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 of TS 34.229-1 [2] applying conditions A5, A8, A11, and A22.

200 OK (Step 11)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 of TS 34.229-1 [2] applying conditions A5, A8, A11, and A22.

ACK (Step 12)

Use the default message "ACK" in Annex A.2.6 of TS 34.229-1 [2] applying conditions A2 and A3.

A.5.2 MTSI MT Voice Call / without preconditions / 5GS

Expected sequence

Step	Direction		Message	Comment
	UE	SS		
1	←		INVITE	SS sends INVITE with the first SDP offer.
2	→		100 Trying	Optional step: UE may send a 100 Trying provisional response.
3	→		183 Session Progress	UE sends 183 Session Progress response reliably, including an SDP answer.
4	←		PRACK	SS acknowledges reception of 183 Session Progress.
5	→		200 OK	UE responds to PRACK.
6	→		180 Ringing	UE sends 180 Ringing.
7	←		PRACK	Conditional step: if UE sent 180 Ringing reliably, SS acknowledges reception of 180 Ringing
8	→		200 OK	Conditional step: if UE sent 180 Ringing reliably, UE responds to PRACK.
9	→		200 OK	UE responds to INVITE.
10	←		ACK	SS acknowledges.
NOTE: The test procedure including NR/5GC signalling is specified in TS 38.508 [21] subclause 4.9.16.				

Specific Message Contents

INVITE (Step 1)

Use the default message "INVITE for MT Call" in Annex A.2.9 of TS 34.229-1 [2] applying conditions A1, A3, and A4, and with 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=-* *c=IN* (addrtype) (connection-address for SS) *b=AS:65* Time description: *t=0 0* Media description: *m=audio* (transport port) *RTP/AVP 96 97 98 99 100* *b=AS:65* *b=RS:0* *b=RR:2000* Attributes for media: *a=rtpmap: 96 EVS/16000* *a=fmtp: 96 br=13.2; bw=swb; max-red=220* *a=rtpmap:97 AMR-WB/16000/1* *a=fmtp:97 mode-change-capability=2; max-red=220* *a=rtpmap: 98 telephone-event/16000* *a=fmtp: 98 0-15* *a=rtpmap:99 AMR/8000/1* *a=fmtp:99 mode-change-capability=2; max-red=220* *a=rtpmap: 100 telephone-event/8000* *a=fmtp: 100 0-15* *a=ptime:20* *a=maxptime:240*

100 Trying (Step 2)

Use the default message "100 Trying for INVITE" in Annex A.2.2 of TS 34.229-1 [2] applying condition A2.

183 Session Progress (Step 3)

Use the default message "183 Session Progress" in Annex A.2.3 of TS 34.229-1 [2] applying condition A2, and with the following exceptions:

Header/param	Value/remark
Status-Line Reason-Phrase	Not checked
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) *EVS/16000* [Note 2] *a=fmtp:*(format) *br=13.2; bw=swb; max-red=220* Note 1: At least one "c=" field shall be present. Note 2: The value for fmt, payload type and format is not checked

PRACK (Step 4)

Use the default message "PRACK" in Annex A.2.4 of TS 34.229-1 [2] applying condition A3.

200 OK (Step 5)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 of TS 34.229-1 [2] applying conditions A5, A8, A11, and A22.

180 Ringing (Step 6)

Use the default message "180 Ringing for INVITE" in Annex A.2.6 of TS 34.229-1 [2] applying conditions A2 and A14, and with the following exceptions:

Header/param	Value/remark
Content-Type media-type	Header not present
Content-Length value	header shall be present if UE uses TCP to send this message and if there is a message body 0
Message-body	Not present

PRACK (Step 7)

Use the default message "PRACK" in Annex A.2.4 of TS 34.229-1 [2] applying condition A3.

200 OK for PRACK (Step 8)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 of TS 34.229-1 [2] applying conditions A5, A8, A11, and A22.

200 OK for INVITE (Step 9)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 of TS 34.229-1 [2] applying conditions A5, A8, A11, and A22.

ACK (Step 10)

Use the default message "ACK" in Annex A.2.6 of TS 34.229-1 [2] applying conditions A2 and A3.

A.6 IMS Emergency Voice Call / 5GS

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 of TS 34.229-1 [2] with condition A28 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] **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: EVS codec shall be present in the media attributes, optionally including channel number "/1".

180 Ringing for INVITE (Step 3)

Use the default message "180 Ringing for INVITE" in Annex A.2.6 of TS 34.229-1 [2] with conditions A4 and A13.

200 OK for INVITE (Step 4)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in Annex A.3.1 of TS 34.229-1 [2] with conditions A6 and A22 and 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. **Session description:** *v=0* *o=- 1111111111 1111111111 IN (addrtype) (unicast-address for SS)* *s=-* *c=IN (addrtype) (connection-address for SS)* *b=AS:37* **Time description:** *t=0 0* **Media description:** *m=audio* (*transport port) RTP/AVP (fmt) [Note 1]* *b=AS:37* *b=RS:0* *b=RR:0* **Attributes for media:** *a=rtpmap:* (*payload type) EVS/16000/1 [Note 1]* *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.

A.7 MO Release of Voice Call / 5GS

Expected sequence

Step	Direction		Message/Procedure	Comment
	UE	SS		
1	→		BYE	The UE releases the call with BYE
2	←		200 OK	The SS sends 200 OK for BYE

Specific message contents

BYE (Step 1)

Use the default message "BYE" in Annex A.2.8 of TS 34.229-1 [2] with conditions A1 and A8.

200 OK (Step 2)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 of TS 34.229-1 [2] with conditions A2 and A22.

A.8 MT Release of Voice Call / 5GS

Expected sequence

Step	Direction		Message/Procedure	Comment
	UE	SS		
1	←		BYE	The SS releases the call with BYE
2	→		200 OK	The UE sends 200 OK for BYE

Specific message contents

BYE (Step 1)

Use the default message "BYE" in Annex A.2.8 of TS 34.229-1 [2] with conditions A3 and A8.

200 OK (Step 2)

Use the default message "200 OK for other requests than REGISTER or SUBSCRIBE" in annex A.3.1 of TS 34.229-1 [2] with conditions A5, A8, and A22.

A.9 EPS Fallback for Voice Call / 5GS

A.9.1 EPS Fallback for Voice Call / steps before fallback / 5GS

Expected sequence

Step	Direction		Message/Procedure	Comment
	UE	SS		
1	→		INVITE	UE sends INVITE including an SDP offer.
2	←		100 Trying	SS sends a 100 Trying provisional response.
3	←		183 Session Progress	SS sends 183 Session Progress including an SDP answer.
4	→		PRACK	UE acknowledges reception of 183 Session Progress.
5	←		200 OK	SS sends 200 OK for PRACK.

Specific message contents

INVITE (Step 1)

Use the default message "INVITE for MO Call Setup" in Annex A.2.1 of TS 34.229-1 [2] with conditions A1, A3, A4, and A28 and the following exceptions:

Header/param	Value/Remark
Message-body	SDP body present but contents not checked

100 Trying (Step 2)

Use the default message "100 Trying for INVITE" in Annex A.2.2 of TS 34.229-1 [2] with condition A1.

183 Session Progress (Step 3)

Use the default message "183 Session Progress for INVITE" in Annex A.2.3 of TS 34.229-1 [2] with condition A1 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=-* - *c=IN* (addrtype) (connection-address for SS) - *b=AS:37* Time description: - *t=0 0* Media description: - *m=audio* (transport port) *RTP/AVP* (fmt) [Note 1, 4] - *b=AS:37* - *b=RS:0* - *b=RR:2000* Attributes for media: - *a=rtpmap:* (payload type) *AMR-WB/16000/1* [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 3] - *a=crypto:1 AES_CM_128_HMAC_SHA1_80inline:PS1uQCVeeCFCanVmcjkpPywjNWhcYD0mXXtxaVBR|2^20|1:4* [Note 3] Note 1: The value for fmt, payload type (AMR) and format is copied from Step 1. 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 1.

PRACK (Step 4)

Use the default message "PRACK" in Annex A.2.4 of TS 34.229-1 [2] with conditions A1 and A7.

200 OK (Step 5)

Use the default message "200 OK for requests other than REGISTER or SUBSCRIBE" in Annex A.3.1 of TS 34.229-1 [2] with conditions A10 and A22.

A.9.2 EPS Fallback for Voice Call / steps after fallback / 5GS

Expected sequence

Step	Direction		Message/Procedure	Comment
	UE	SS		
1	→		UPDATE	UE sends an UPDATE request containing a second SDP offer.
2	←		200 OK	SS sends a 200 OK response for UPDATE containing an SDP answer.
3	←		180 Ringing	SS sends a 180 Ringing provisional response.
4	←		200 OK	SS responds to INVITE with 200 OK.
5	→		ACK	UE acknowledges.

Specific message contents

UPDATE (Step 1)

Use the default message "UPDATE" in Annex A.2.5 of TS 34.229-1 [2] with conditions A1 and A5 and the following exceptions:

Header/param	Value/Remark
Require option-tag	*precondition* (shall be present if SDP message-body present)
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) [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 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-WB/16000* [Note 2] [Note 4] - *a=fmtp:* (format) [Note 2, 3] 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 Note 4: The AMR channel number shall be “/1” or omitted.

200 OK (Step 2)

Use the default message "200 OK for requests other than REGISTER or SUBSCRIBE" in Annex A.3.1 of TS 34.229-1 [2] with conditions A1, A10 and A21 and the following exceptions:

Header/param	Value/remark
Require option-tag	*precondition* (present if UE uses preconditions)
Content-Type media-type	*application/sdp*
Content-Length Value	length of message-body
Message-body	SDP body of the 200 OK response copied from the received UPDATE and modified as follows: - IP address on "c=" lines and transport port on "m=" lines changed to indicate to which IP address and port the UE should start sending the media; - "o=" line identical to previous SDP sent by SS except that sess-version is incremented.

180 Ringing (Step 3)

Use the default message "180 Ringing for INVITE" in Annex A.2.6 of TS 34.229-1 [2] with conditions A1 and A13.

200 OK (Step 4)

Use the default message "200 OK for requests other than REGISTER or SUBSRIBE" in Annex A.3.1 of TS 34.229-1 [2] with conditions A1, A10, A19, and A21.

ACK (Step 5)

Use the default message "ACK" in Annex A.2.7 of TS 34.229-1 [2] with condition A1.

Annex B (informative): Change history

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
2019-10	RAN5#85	R5-197746	-	-	-	First draft version V0.1.0 made available	0.1.0
2019-11	RAN5#85	R5-198832	-	-	-	Second draft version V0.2.0 made available, implementing pCRs R5-197934, R5-198899, R5-198239, R5-198240, and R5-198241	0.2.0
2020-06	RAN5#87-e	R5-201458	-	-	-	Third draft version V0.3.0 made available, implementing pCRs R5-202693, R5-202686, R5-202687, R5-202688, R5-202689, R5-202678, R5-202679, R5-202680, R5-202681, R5-202682, R5-202690, R5-202683, R5-202684, R5-202685, R5-202691, R5-202692	0.3.0
2020-06	RAN5#87-e	-	-	-	-	Raised to v15.0.0	15.0.0
2020-09	RAN5#88-e	R5-203437	0004	-	F	Corrections to A.2 on IMS Registration	15.1.0
2020-09	RAN5#88-e	R5-203439	0006	-	F	New generic procedure for MT Call Release	15.1.0
2020-09	RAN5#88-e	R5-203440	0007	-	F	Adding references as needed	15.1.0
2020-09	RAN5#88-e	R5-203441	0008	-	F	Corrections to test cases 7.6 and 7.7	15.1.0
2020-09	RAN5#88-e	R5-203442	0009	-	F	Corrections to test case 6.1	15.1.0
2020-09	RAN5#88-e	R5-203443	0010	-	F	Corrections to test case 6.2	15.1.0
2020-09	RAN5#88-e	R5-203445	0012	-	F	Corrections to test case 6.4	15.1.0
2020-09	RAN5#88-e	R5-203447	0013	-	F	Corrections to test case 6.5	15.1.0
2020-09	RAN5#88-e	R5-203448	0014	-	F	Corrections to test case 6.6	15.1.0
2020-09	RAN5#88-e	R5-203452	0015	-	F	Corrections to test case 6.7	15.1.0
2020-09	RAN5#88-e	R5-203453	0016	-	F	Corrections to test case 6.8	15.1.0
2020-09	RAN5#88-e	R5-203454	0017	-	F	Corrections to test case 6.9	15.1.0
2020-09	RAN5#88-e	R5-203461	0018	-	F	Corrections to MTSI MT Voice Call TC 7.6	15.1.0
2020-09	RAN5#88-e	R5-203462	0019	-	F	Corrections to Annex A.5.1	15.1.0
2020-09	RAN5#88-e	R5-204477	0001	1	F	Addition of IMS NR TC 9.4-MT Concatenated SMS	15.1.0
2020-09	RAN5#88-e	R5-204478	0002	1	F	Addition of IMS NR TC 9.5-MO SMS RP-ERROR	15.1.0
2020-09	RAN5#88-e	R5-204479	0003	1	F	Addition of IMS NR TC 10.1-emergency call with registration and Location	15.1.0
2020-09	RAN5#88-e	R5-204480	0005	1	F	Adding details for A.3 for IMS Emergency Registration	15.1.0
2020-09	RAN5#88-e	R5-204481	0011	1	F	Corrections to test case 6.3	15.1.0
2020-09	RAN5#88-e	R5-204482	0020	1	F	Addition of new IMS 5GS test case 9.1	15.1.0
2020-09	RAN5#88-e	R5-204483	0021	1	F	Addition of new IMS 5GS test case 9.2	15.1.0
2020-09	RAN5#88-e	R5-204484	0022	1	F	New generic IMS procedures for use in EPS fallback	15.1.0
2020-09	RAN5#88-e	R5-204485	0023	1	F	Addition of NR TC 8.18 Barring of All Incoming Calls / except for a specific user / 5GS	15.1.0
2020-09	RAN5#88-e	R5-204486	0024	1	F	Addition of NR TC 9.3 Mobile Originating Concatenated SMS / 5GS	15.1.0
2020-09	RAN5#88-e	R5-204487	0026	1	F	Addition of new IMS test case 8.1	15.1.0

History

Document history		
V15.0.0	August 2020	Publication
V15.1.0	November 2020	Publication