ETSI TS 103 389 V2.0.0 (2014-08)

**Railway Telecommunications (RT);
Global System for Mobile communications (GSM);
Usage of Session Initiation Protocol (SIP) on the
Network Switching Subsystem (NSS) to Fixed Terminal
Subsystem (FTS) interface for GSM Operation on Railways**

Reference
RTS/RT-00014

Keywords
GSM-R, railways

ETSI

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

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

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

Important notice

The present document can be downloaded from:
http://www.etsi.org

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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

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

Contents

Intellectual Property Rights

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Railway Telecommunications (RT).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**may not**", "**need**", "**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.

Introduction

While a number of interoperability specifications for various interfaces at various layers of GSM-R systems exist, the interface between the Network Switching Subsystem (NSS) and the Fixed Terminal Subsystem (FTS) has not yet been addressed by any interoperability specification activity.

In most of the GSM-R system deployments available at the time of the creation of the present document, the Network Switching Subsystem and the Fixed Terminal Subsystem are interconnected using TDM based interfaces such as DSS1 [i.2].

TS 102 610 [9] specifies the usage and format of UUIE for call-related end-to-end functionality in GSM-R systems but no other interworking topics.

The present document addresses the interoperability specification gap between the Network Switching Subsystem and the Fixed Terminal Subsystem with an interface based on the Internet Protocol (IP) [2], the Session Initiation Protocol (SIP) [3], the Session Description Protocol (SDP) [6] and the Real-Time Transport Protocol (RTP) [7].

In addition to the table of contents, the following explanation will help you navigate through and understand the contents of the present document:

- Clauses 1 to 3 are predefined by ETSI.
- Clause 4 shows and explains the reference system architecture and identifies the interface(s) for the present document.
- Clause 5 holds the functional requirements for the interface subject to the present document.
- Clause 6 specifies in detail the signalling interface for all supported functions and services.
- Clause 7 specifies in detail the media interface.

- Clause 8 specifies the additions and changes for a voice recorder interface.
- Annex A explains the mechanism to locate SIP entities at the present interface.
- Annex B contains recommendations on the use and implementation of standardized Quality of Service mechanisms at the present interface.
- Annex C contains recommendations about the security mechanisms.
- Annex D contains a mapping table of EIRENE [1] to interface features.

1 Scope

The present document defines the signalling and media interface between the Network Switching Subsystem and the Fixed Terminal Subsystem in order to provide a clear set of services needed for GSM-R operations. This includes voice call service and available call-related supplementary services. The present document addresses the Internet Layer and upwards of the Internet Protocol Suite [i.18] on the signalling and media interface.

Any service other than voice call service and call-related supplementary services (such as data services, Short Message Service, etc.) is out of scope of the present document; additional features may be addressed in future releases.

The present document does not specify any other interface between the Network Switching Subsystem and the Fixed Terminal Subsystem nor does it cover any internal interfaces of either NSS or FTS. Voice recording and related interfaces are out of scope of the present document. Such interfaces may be addressed in a future release of the present document.

The present document does not address any specific 3GPP Release or Architecture.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] UIC P001D010 (Version 15.1): "UIC Project EIRENE System Requirements Specification".

NOTE: Available at http://www.uic.org/IMG/pdf/eirene_srs_15.1.pdf.

[2] IETF RFC 791 (1981): "Internet Protocol".

[3] IETF RFC 3261 (2002): "SIP: Session Initiation Protocol".

[4] IETF RFC 3264 (2002): "An Offer/Answer Model Session Description Protocol (SDP)".

[5] IETF RFC 4733 (2006): "RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals".

[6] IETF RFC 4566 (2006): "SDP: Session Description Protocol".

[7] IETF RFC 3550 (2003): "RTP: A Transport Protocol for Real-Time Applications".

[8] IETF RFC 3326 (2002): "The Reason Header Field for the Session Initiation Protocol (SIP)".

[9] ETSI TS 102 610 (V1.1.0): "Railways Telecommunications (RT); Global System for Mobile communications (GSM); Usage of the User to User Information Element for GSM Operation on Railways".

[10] IETF RFC 5234 (2008): "Augmented BNF for Syntax Specifications: ABNF".

[11] IETF RFC 3262 (2002): "Reliability of Provisional Responses in Session Initiation Protocol (SIP)".

[12] IETF RFC 4412 (2006): "Communications Resource Priority for the Session Initiation Protocol (SIP)".

[13] IETF RFC 3325 (2002): "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks".

[14] IETF RFC 5876 (2010): "Updates to Asserted Identity in the Session Initiation Protocol (SIP)".

[15] IETF RFC 3323 (2002): "A Privacy Mechanism for the Session Initiation Protocol (SIP)".

[16] IETF RFC 4028 (2005): "Session Timers in the Session Initiation Protocol (SIP)".

[17] IETF RFC 3311 (2002): "The Session Initiation Protocol (SIP) UPDATE Method".

[18] IETF RFC 2474 (1998): "Definitions of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers".

[19] IETF RFC 2475 (1998): "An Architecture for Differentiated Services".

[20] IETF RFC 4594 (2006): "Configuration Guidelines for DiffServ Service Classes".

[21] IETF RFC 5865 (2010): "A Differentiated Services Code Point (DSCP) for Capacity-Admitted Traffic".

[22] Recommendation ITU-T Q.850 (1998): "Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN user part".

[23] Recommendation ITU-T E.164 (2010): "The international public telecommunication numbering plan".

[24] Recommendation ITU-T Q.955.3 (1993): "Stage 3 description for community of interest supplementary services using DSS 1: Multi-level precedence and preemption (MLPP)".

[25] IETF RFC 3986 (2005): "Uniform Resource Identifier (URI): Generic Syntax".

[26] IETF RFC 768 (1980): "User Datagram Protocol".

[27] Recommendation ITU-T G.711 (1988): "Pulse code modulation (PCM) of voice frequencies".

[28] IETF RFC 2833 (2000): "RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals".

[29] IETF RFC 5009 (2007): "Private Header (P-Header) Extension to the Session Initiation Protocol (SIP) for Authorization of Early Media".

[30] IETF RFC 3840 (2004): "Indicating User Agent Capabilities in the Session Initiation Protocol (SIP)".

[31] IETF RFC 4574 (2006): "The Session Description Protocol (SDP) Label Attribute".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] IETF draft RFC draft-johnston-cuss-sip-uui-01: "A Mechanism for Transporting User to User Call Control Information in SIP".

[i.2] ETSI ETS 300 403-1 (V1.3.2): "Integrated Services Digital Network (ISDN); Digital Subscriber Signalling System No. one (DSS1) protocol; Signalling network layer for circuit-mode basic call control; Part 1: Protocol specification [ITU-T Recommendation Q.931 (1993), modified]".

[i.3] IETF RFC 6086 (2011): "Session Initiation Protocol (SIP) INFO Method and Package Framework".

[i.4] IETF RFC 3428 (2002): "Session Initiation Protocol (SIP) Extension for Instant Messaging".

[i.5] IETF RFC 3515 (2001): "The Session Initiation Protocol (SIP) Refer Method".

[i.6] IETF RFC 3265 (2002): "Session Initiation Protocol (SIP)-Specific Event Notification".

[i.7] IETF RFC 3903 (2004): "Session Initiation Protocol (SIP) Extension for Event State Publication".

[i.8] IETF RFC 1594 (1994): "FYI on Questions and Answers to Commonly asked "New Internet User" Questions".

[i.9] IETF RFC 3665 (2003): "Session Initiation Protocol (SIP) Basic Call Flow Examples".

[i.10] IETF RFC 3960 (2004): "Early Media and Ringing Tone Generation in the Session Initiation Protocol (SIP)".

[i.11] ETSI EN 300 925 (V7.0.2): "Digital cellular telecommunications system (Phase 2+) (GSM); Voice Group Call Service (VGCS) - Stage 1 (GSM 02.68 version 7.0.2 Release 1998)".

[i.12] ETSI EN 300 926 (V8.0.1): "Digital cellular telecommunications system (Phase 2+) (GSM); Voice Broadcast Service (VBS) - Stage 1 (GSM 02.69 version 8.0.1 Release 1999)".

[i.13] IETF RFC 3263 (2002): "Session Initiation Protocol (SIP): Locating SIP Servers".

[i.14] IETF RFC 1035 (1987): "Domain names - implementation and specification".

[i.15] IETF RFC 2181 (1997): "Clarifications to the DNS Specification".

[i.16] IETF RFC 2663 (1999): "IP Network Address Translator (NAT) Terminology and Considerations".

[i.17] Recommendation ITU-T I.255.3 (1990): "Multi-Level Precedence and Pre-emption service".

[i.18] IETF RFC 1122 (1989): "Requirements for Internet Hosts -- Communication Layers".

[i.19] IETF RFC 3551: "RTP Profile for Audio and Video Conferences with Minimal Control".

[i.20] IETF draft RFC draft-portman-siprec-protocol-12: "Session Recording Protocol draft-ietf-siprec-protocol-12".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

call: refers to a SIP Dialog (RFC 3261 [3]) between two Signalling Endpoints, established for the purpose of a voice communication and related data exchange

client: As defined in RFC 3261 [3].

Communication Session (CS): session that is the subject of recording

dialog: As defined in RFC 3261 [3].

final response: As defined in RFC 3261 [3].

Fixed Terminal Subsystem (FTS): part of the EIRENE [1] system that provides access to this network (and services) via controller equipment (in general referred to as Fixed Terminals)

Fully Qualified Domain Name (FQDN): As defined in RFC 1594 [i.8].

header: As defined in RFC 3261 [3].

header field: As defined in RFC 3261 [3].

initiator, calling party, caller: As defined in RFC 3261 [3].

invitee, invited user, called party, callee: As defined in RFC 3261 [3].

Media Endpoint, RTP Endpoint: entity that terminates RTP stream(s) under the control of a single SIP Endpoint in the same subsystem

NOTE: This entity may be physically separated from the SIP Endpoint.

method: As defined in RFC 3261 [3].

Network Switching Subsystem (NSS): part of the PLMN infrastructure that performs all necessary functions in order to handle the call services to and from the mobile stations as well as to and from fixed terminals

operational priority: as defined in EIRENE SRS [1] different call types have call priorities during railway communications. This behaviour is mentioned as operational priority of a call

option tag: As defined in RFC 3261 [3].

provisional response: As defined in RFC 3261 [3].

proxy, proxy server: As defined in RFC 3261 [3].

Recording Session (RS): SIP session created between SRC and SRS for the purpose of recording a Communication Session

request: As defined in RFC 3261 [3].

response: As defined in RFC 3261 [3].

server: As defined in RFC 3261 [3].

session: As defined in RFC 3261 [3].

Signalling Endpoint, SIP Endpoint: entity that acts as a SIP User Agent

NOTE: Within the scope of the present document this term refers to NSS and FTS.

Signalling Proxy, SIP Proxy: Proxy Server as defined by RFC 3261 [3]

(SIP) transaction: As defined in RFC 3261 [3].

tag: As defined in RFC 3261 [3].

User Agent Client (UAC): As defined in RFC 3261 [3].

User Agent Server (UAS): As defined in RFC 3261 [3].

User Agent (UA): As defined in RFC 3261 [3].

3.2 Abbreviations

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

ACK	ACKnowledgement
AF	Assured Forwarding
AoCC	Advice of Charge (Charging)
AoCI	Advice of Charge (Information)
B2BUA	Back to Back User Agent
BAIC	Barring of All Incoming Calls
BAOC	Barring of All Outgoing Calls
BIC-Roam	Barring of Incoming Calls when Roaming Outside the Home PLMN Country
BNF	Backus Naur Form
BOIC	Barring of Outgoing International Calls
BOIC-exHC	BOIC except those to Home PLMN Country
CCBS	Completion of Calls to Busy Subscribers

CFB	Call Forwarding on Mobile Subscriber Busy
CFNRc	Call forwarding on Mobile Subscriber Not Reachable
CFNRy	Call Forwarding on No Reply
CFU	Call Forwarding Unconditional
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CN	Core Node
CoLP	Connected Line Identification Presentation
CoLR	Connected Line Identification Restriction
CS	Communication Session
CSRC	Contributing SouRCe
CUG	Closed User Group
CW	Call waiting
DL	Down Link
DNS	Domain Name Service
DSCP	Differentiated Service Code Point
DTMF	Dual Tone Multi Frequency
ECT	Explicit Call Transfer
EF	Expedited Forwarding
EIRENE	European Integrated Railway Radio Enhanced Network
eMLPP	enhanced Multi-Level Precedence and Pre-emption
FQDN	Fully Qualified Domain Name
FTS	Fixed Terminal Subsystem
GSM-R	Global System Mobile-Railways
HOLD	Call hold
IN	Intelligent Network
IP	Internet Protocol
MLPP	Multi-Level Precedence and Pre-emption
MO/PP	Mobile Originated/Point-to-Point
MPTY	Multi Party Service
MT/PP	Mobile Terminated/Point-to-Point
NAPT	Network Address Port Translation
NAT	Network Address Translation
NSS	Network Switching Subsystem
OSI	Open Systems Interconnection
PABX	Private Access Branch eXchange
PCM	Pulse Code Modulation
PHB	Per Hop Behaviour
PLMN	Public Land Mobile Network
PRA	PRovisional Acknowledgment
PRACK	Provisional Response Acknowledgement
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RFC	Request For Comments
RS	Recording Session
RTP	Real-Time Transport Protocol
SDP	Session Description Protocol
SE	Session Expires
SIP	Session Initiation Protocol
SRC	Session Recording Client
SRS	Session Recording Server
SRTP	Secured Real-time Protocol
SSRC	Synchronisation SouRCe
TDM	Time Division Multiplexing
ToS	Type of Service
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UIC	Union Internationale des Chemins de Fer, International Union of Railways
URI	Uniform Resource Identifier
URN	Uniform Resource Name

USSD	Unstructured Supplementary Service Data
UUI	User-to-User Information
UUIE	User to User Information Element
UUS1	User-to-User Signalling 1
VBS	Voice Broadcast Service
VGCS	Voice Group Call Service

4 Reference System Architecture

The system architecture used to identify the interface that is the subject of the present document is a simplification of a GSM-R system down to a minimum of logical entities relevant to the present document.

Within the context of the present document a GSM-R system is logically divided into a GSM-R Network and a Fixed Terminal Subsystem. The interface between the Mobile Terminals and the NSS as well as the interface between the Fixed Terminals and the FTS are explicitly not addressed in the present document. The focus of the present document is solely:

- the Signalling Interface; and
- the Media Interface;

between the logical subsystem NSS and the logical subsystem FTS.

It is important to note that this architecture does not necessarily reflect any physical entities in a GSM-R system.

Figure 4.1 illustrates the reference system architecture.

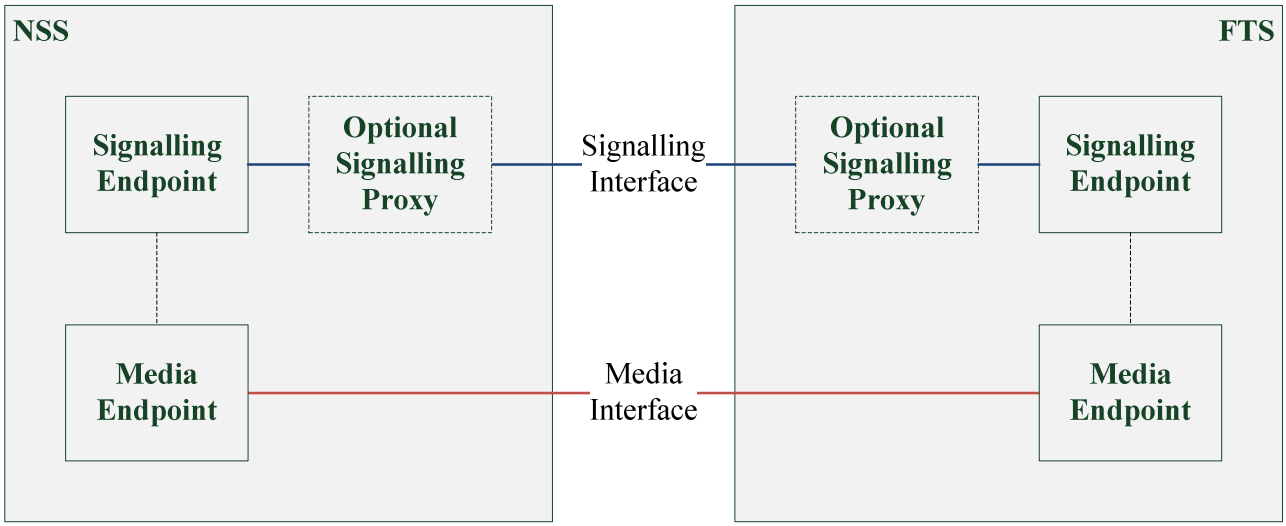


Figure 4.1: Reference System Architecture

Depending on the deployment scenario and the NSS/FTS design there may be one or more Signalling Endpoints, one or more Media Endpoints and zero or more Signalling Proxies on either side of the interface.

The Media Endpoint(s) are controlled by (a) Signalling Endpoint(s) in the same subsystem. This control mechanism is out of scope of the present document.

One Signalling Endpoint may establish more than one call. Also one Signalling Proxy and one Media Endpoint may be involved in one or more calls.

The maximum number of Signalling Endpoints allowed to be involved in a single call on the present interface is two-one on each side.

Optionally deployed Signalling Proxies may be involved in the signalling flow for either incoming traffic or outgoing traffic or both incoming and outgoing traffic at either side of the interface. This depends on the FTS/NSS design and the deployment scenario. The entities involved might differ depending on the call direction, but have to be the same for all calls in the same direction in a single deployment scenario.

Annex A includes several deployment scenario examples that illustrate some of the Signalling Proxy deployment options.

5 Interface Functionality

This clause specifies functional requirements of the interface. The technical details are specified in clauses 6 and 7 of the present document.

5.1 Basic Call

The primary function to be delivered by the present interface is the means to initiate and tear down full duplex audio (voice) connections between the NSS and FTS with a single, logical, SIP Endpoint involved per connection on each side of the present interface that controls the connection as well as its respective Media Endpoint (compare clause 4).

Such a connection can be initialized by either NSS or FTS. The initiation phase shall specifically provide means and mechanisms for per call/connection capability exchange, media negotiation, progress indication as well as error indication and handling.

5.1.1 Progress Indication

Progress indication shall be provided via explicit signalling. In addition a progress tone generation policy, clearly stating which party shall generate which progress tones and when, is defined.

5.1.2 Early Media

Furthermore, the basic call procedure shall provide a means for media (i.e. audio) exchange prior to call setup completion. This shall be possible in the direction callee to caller only. This functionality is needed in order to provide pre-call announcements to the user before the dialog is established.

5.2 Connected Parties Identity Information

The calling party shall provide its identity information with the connection request.

The calling party shall be informed about the identity of the remote party.

The identity information shall contain a routable number in the underlying network's address space and in addition - if available - an EIRENE functional number.

Upon change of identity of either connected party an immediate identity update shall be transmitted to the other side.

5.3 Call Hold

Both endpoints of an established call shall be able to suspend an associated media stream and resume it at a later time. The endpoint holding the call shall inform the other party that the call is suspended and shall further inform the other party when the call is reconnected. The media stream is not just interrupted, but possibly redirected to some other source which generates, for example, an announcement or "music on hold".

5.4 Multi Level Precedence and Pre-emption

In order to allow differentiated/preferred treatment of calls of different/higher operational priority (e.g. emergency calls) when facing resource limits, the interface shall support signalling mechanisms and procedures to provide multi level precedence signalling and as well as call pre-emption functionality. Additionally, MLPP is used by the Signalling Endpoints to handle different priorities at the operational level. In particular this includes flagging of session priority and signalling flows for precedence blocking as well as pre-emption of calls, but not for reservation of resources.

The present document defines how call precedence and pre-emption is performed, but it does not define the algorithm that causes precedence blocking or call pre-emption to be performed.

5.5 Voice Group Call and Broadcast Call Control

Voice Group Calls [i.11] and Voice Broadcast Calls [i.12] are service implementations in the NSS.

The interface subject to the present document shall provide mechanisms for the FTS to control voice group calls and voice broadcast calls from the perspective of Fixed Terminal users as defined by EIRENE [1]. Control of voice group calls and voice broadcast calls from the perspective of other users is out-of-scope of the present document.

The following control mechanisms shall be supported on the present interface:

- Termination ("kill") of VGCS/VBS calls.
- Requests for muting and unmuting of the mobile terminal downlink of VGCS calls.

When an FTS subscriber is involved in such a call then it is connected by means of a point to point call on the present interface. The VGCS/VBS call is identified at the application level purely on the basis of the NSS subscriber number contained in the call signalling.

5.6 User-User-Information-Element Transport

User-to-User-Information-Elements (UUIE) [i.2] are used in GSM-R systems to carry EIRENE specific information and are exchanged within basic call control messages. TS 102 610 [9] specifies in detail the use and content of UUIEs in GSM-R and also distinguishes between international and national EIRENE UUIE tags.

The interface subject to the present document shall support a mechanism to transparently transport the content of the UUIE specified by TS 102 610 [9]. The transport of international and national tags and their values shall be supported.

5.7 Reason Transport

In most currently deployed GSM-R systems fixed and mobile terminals make use of end-to-end release cause signalling.

The present interface shall therefore support the transparent, end-to-end transport of release and disconnect reasons between the fixed terminals and GSM-R mobile terminals and vice versa.

6 Signalling Interface

6.1 Network Layer Protocol

NSS and FTS shall use IPv4 [2] as the network layer protocol.

Network Address Translation (NAT) is a method used for IP address translation between address realms. NAT adds complexity to higher layer protocols that is not dealt with in the present document. Therefore no form of NAT shall be implemented in the network infrastructure at the signalling interface. See RFC 2663 [i.16] for more information on NAT.

6.2 Transport Layer Protocol

NSS and FTS shall use UDP RFC 768 [26] as the transport layer protocol.

Network Address and Port Translation (NAPT) is a form of NAT that extends to the transport layer. For the same reason as for pure network layer NAT, NAPT shall not be implemented in the network infrastructure at the signalling interface. See RFC 2663 [i.16] for more information on NAPT.

6.3 Signalling Protocol

NSS and FTS shall support SIP in accordance with:

- RFC 3261 [3];

and SDP in accordance with:

- RFC 4566 [6]; and
- RFC 3264 [4];

as signalling protocols further qualified by statements in later clauses of the present document.

Requirements for support of other IETF RFCs and other standards are as stated in later clauses of the present document.

Deviations from and/or limited applicability of those RFCs are explicitly pointed out where appropriate.

6.3.1 SIP Entities

A SIP network can be composed of many logical SIP entities. Each entity provides specific functions and participates in SIP communication as a client (initiates requests), as a server (responds to requests), or as both. One physical entity can implement the functionality of more than one logical SIP entity.

On the interface subject to the present document the allowed, and therefore relevant, SIP entities are SIP User Agents (UAs) and SIP Proxy Servers, both defined in RFC 3261 [3].

Depending on the FTS and NSS implementation the interaction at the interface may be performed:

- directly between a SIP User Agent and a SIP User Agent; or
- between a SIP User Agent, one or more SIP Proxy Servers and a SIP User Agent.

6.3.1.1 SIP User Agent

UAs initiate and terminate sessions by exchanging requests and responses. RFC 3261 [3] defines a User Agent as a logical entity that can act both as User Agent Client and as User Agent Server. User Agent Client and User Agent Server are defined in RFC 3261 [3].

In a SIP environment a SIP User Agent (UA) is a Signalling Endpoint. Therefore on the present interface every connection is terminated by one SIP UA on either side of the interface.

Which physical entities represent the SIP UAs are subject to the subsystem design of the NSS and FTS.

6.3.1.2 SIP Proxy

A Proxy Server is defined in RFC 3261 [3].

The deployment of SIP Proxy Servers on either side of the present interface is optional and subject to the FTS/NSS design.

A typical application probably requiring the use of a SIP Proxy at the present interface may be a load balancing service in front of a number of Signalling Endpoints.

As implicitly required by the reference system architecture in clause 4 of the present document, a SIP Proxy at the present interface shall not perform parallel forking as defined in RFC 3261 [3] as this would increase the number of Signalling Endpoints involved in a single dialog. If such functionality is required at a system level it shall be implemented and hidden within the FTS and/or NSS.

6.3.2 SIP Request Methods

Table 6.1 specifies the requests that shall be, may be, or shall not be, supported by the SIP entities on the present interface in order to provide the required interface functionality. The terms and abbreviations used in table 6.1 have the following meaning:

"Sending" means "initiating the method"

"Replying" means "answering the method with an appropriate response"

"Proxying" means "Forwarding the method to another SIP entity"

"m" means "Mandatory"

"o" means "Optional"

"x" means "Not allowed"

"n/a" means "Not applicable"

Table 6.1: Supported SIP Methods

Method	Reference	SIP Entity				
		User Agent		Proxy Server		
		Sending	Replying	Sending	Replying	Proxying
INVITE	RFC 3261 [3]	m	m	c (see note 1)	o (see note 2)	m
ACK	RFC 3261 [3]	m	n/a	n/a	n/a	m
CANCEL	RFC 3261 [3]	m	m	n/a	n/a	m
BYE	RFC 3261 [3]	m	m	o (see note 3)	n/a	m
OPTIONS	RFC 3261 [3]	o	m	o	m	m
PRACK	RFC 3262 [11]	m	m	n/a	n/a	m
UPDATE	RFC 3311 [17]	o	m	n/a	n/a	m
REGISTER	RFC 3261 [3]	x	x	x	x	x
INFO	RFC 6086 [i.3]	m	m	n/a	n/a	m
MESSAGE	RFC 3428 [i.4]	x	x	x	x	x
REFER	RFC 3515 [i.5]	x	x	x	x	x
NOTIFY	RFC 3265 [i.6]	x	x	x	x	x
SUBSCRIBE	RFC 3265 [i.6]	x	x	x	x	x
PUBLISH	RFC 3903 [i.7]	x	x	x	x	x
NOTE 1: Conditional, a proxy server is allowed to send an INVITE method in some circumstances (e.g. serial forking) but only if no new dialog is established. NOTE 2: The only response a proxy server may generate and send is 100 Trying. NOTE 3: Is only allowed in case of session timeout.						

6.3.3 SIP Responses

Upon receiving a SIP request SIP entities reply to it with an appropriate SIP response, which depends on the type of request, the type of the receiving SIP entity and the request computing logic.

All SIP entities implementing the present interface shall support sending, receiving and processing of all applicable response codes defined in RFC 3261 [3], RFC 4412 [12] and RFC 4028 [16] and use them in accordance with the respective description in RFC 3261 [3], RFC 4412 [12] and RFC 4028 [16].

6.3.4 SIP Header Fields

RFC 3261 [3], RFC 3262 [11], RFC 3326 [8], RFC 4412 [12], RFC 3325 [13], RFC 5876 [14], RFC 3323 [15], RFC 4028 [16], RFC 3311 [17], RFC 5009 [29] and RFC 6086 [i.3] - all of them are applicable to the present interface - specify in detail the SIP header fields used at the present interface and explain their respective usage.

General rules for processing SIP header fields are defined in RFC 3261 [3] and fully apply to the present interface.

Table 6.2 summarizes the usage of SIP header fields at the present interface. The table legend can be found in RFC 3261 [3], section 20.

Additional information is encoded in the cell background colour:

- "Grey" cells indicate that the usage pattern on the present interface is the same as that of the original RFC definition.
- "White" cells indicate that the usage pattern at the present interface is different from the original RFC definition.

Table 6.2: Summary of SIP Header Fields

Header field	Reference	Where	Proxy	ACK	BYE	CAN	INV	OPT	PRA	UPD	INF
Accept	RFC 3261 [3]	R		-	o	-	o	m*	o	o	o
Accept	RFC 3261 [3]	2xx		-	-	-	o	m*	-	o	-
Accept	RFC 3261 [3]	415		-	c	-	c	c	c	c	o
Accept-Encoding	RFC 3261 [3]	R		-	o	-	o	o	o	o	o
Accept-Encoding	RFC 3261 [3]	2xx		-	-	-	o	m*	-	o	o
Accept-Encoding	RFC 3261 [3]	415		-	c	-	c	c	c	c	c
Accept-Language	RFC 3261 [3]			-	-	-	-	-	-	-	-
Accept-Resource-Priority	RFC 4412 [12]			-	-	-	-	-	-	-	-
Alert-Info	RFC 3261 [3]			-	-	-	-	-	-	-	-
Allow	RFC 3261 [3]	R		-	o	-	o	o	o	o	o
Allow	RFC 3261 [3]	2xx		-	o	-	m*	m*	o	o	-
Allow	RFC 3261 [3]	r		-	o	-	o	o	o	o	o
Allow	RFC 3261 [3]	405		-	m	-	m	m	m	m	m
Authentication-Info	RFC 3261 [3]			-	-	-	-	-	-	-	-
Authorization	RFC 3261 [3]			-	-	-	-	-	-	-	-
Call-ID	RFC 3261 [3]	c	r	m	m	m	m	m	m	m	m
Call-Info	RFC 3261 [3]		ar	-	-	-	o	o	-	o	o
Contact	RFC 3261 [3]	R		o	-	-	m	o	-	m	-
Contact	RFC 3261 [3]	1xx		-	-	-	o	-	-	o	-
Contact	RFC 3261 [3]	2xx		-	-	-	m	o	-	m	-
Contact	RFC 3261 [3]	3xx	d	-	o	-	o	o	o	o	-
Contact	RFC 3261 [3]	485		-	o	-	o	o	o	o	-
Content-Disposition	RFC 3261 [3]			o	o	-	o	o	o	o	o
Content-Encoding	RFC 3261 [3]			o	o	-	o	o	o	o	o
Content-Language	RFC 3261 [3]			-	-	-	-	-	-	-	-
Content-Length	RFC 3261 [3]		ar	t	t	t	t	t	t	t	t
Content-Type	RFC 3261 [3]			*	*	-	*	*	*	*	*
CSeq	RFC 3261 [3]	c	r	m	m	m	m	m	m	m	m
Date	RFC 3261 [3]		a	o	o	o	o	o	o	o	o
Error-Info	RFC 3261 [3]	300-699		-	-	-	-	-	-	-	-
Expires	RFC 3261 [3]			-	-	-	-	-	-	-	-
From	RFC 3261 [3]	c	r	m	m	m	m	m	m	m	m
In-Reply-To	RFC 3261 [3]	R		-	-	-	o	-	-	-	-
Info-Package	RFC 6086 [i.3]	R		-	-	-	-	-	-	-	m*
Max-Forwards	RFC 3261 [3]	R	amr	m	m	m	m	m	m	m	o
MIME-Version	RFC 3261 [3]			o	o	-	o	o	o	o	o
Min-Expires	RFC 3261 [3]	423		-	-	-	-	-	-	-	-
Min-SE	RFC 4028 [16]	R	amr	-	-	-	o	-	-	o	-
Min-SE	RFC 4028 [16]	422		-	-	-	m	-	-	m	-
Organization	RFC 3261 [3]			-	-	-	-	-	-	-	-
P-Asserted-Identity	RFC 3325 [13] RFC 5876 [14]		r	-	o	-	o	o	o	o	-
P-Preferred-Identity	RFC 3325 [13] RFC 5876 [14]			-	-	-	-	-	-	-	-
Priority	RFC 3261 [3]			-	-	-	-	-	-	-	-

Header field	Reference	Where	Proxy	ACK	BYE	CAN	INV	OPT	PRA	UPD	INF
Privacy	RFC 3323 [15]		r	o	o	o	o	o	o	o	o
Proxy-Authenticate	RFC 3261 [3]			-	-	-	-	-	-	-	-
Proxy-Authorization	RFC 3261 [3]			-	-	-	-	-	-	-	-
Proxy-Require	RFC 3261 [3]	R	ar	-	o	-	o	o	o	o	o
User-to-User	The present document	R	r	-	o	-	o	-	-	-	o
User-to-User	The present document	r	r	-	-	-	o	-	-	-	o
RAck	RFC 3262 [11]	R		-	-	-		-	m	-	-
Reason	RFC 3326 [8]	R	r	-	o	o	-	-	-	-	-
Reason	RFC 3326 [8]	r	r	-	-	-	o	-	-	-	-
Record-Route	RFC 3261 [3]	R	ar	o	o	o	o	o	o	o	o
Record-Route	RFC 3261 [3]	2xx,18x	mr	-	o	o	o	o	o	o	o
Recv-Info	RFC 6086 [i.3]	R		-	-	-	o	-	o	o	-
Recv-Info	RFC 6086 [i.3]	2xx		-	-	-	o	-	o	o	-
Recv-Info	RFC 6086 [i.3]	1xx		-	-	-	o	-	-	-	-
Recv-Info	RFC 6086 [i.3]	469		-	-	-	-	-	-	-	m*
Recv-Info	RFC 6086 [i.3]	r		-	-	-	o	-	o	o	-
Reply-To	RFC 3261 [3]			-	-	-	-	-	-	-	-
Require	RFC 3261 [3]		r	-	-	-	m	m	-	m	o
Resource-Priority	RFC 4412 [12]	R	r	-	-	-	m	-	-	-	-
Retry-After	RFC 3261 [3]	404,413,480, 486,500,503, 600,603		-	o	o	o	o	o	o	o
Route	RFC 3261 [3]	R	adr	c	c	c	c	c	c	c	o
RSeq	RFC 3262 [11]	1xx		-	-	-	m	-	-	-	-
Server	RFC 3261 [3]	r		-	o	o	o	o	o	o	o
Session-Expires	RFC 4028 [16]	R	amr	-	-	-	o	-	-	o	-
Session-Expires	RFC 4028 [16]	2xx	ar	-	-	-	o	-	-	o	-
Subject	RFC 3261 [3]	R		-	-	-	-	-	-	-	-
Supported	RFC 3261 [3]	R		-	o	o	m*	o	o	o	o
Supported	RFC 3261 [3]	2xx		-	o	o	m*	m*	o	o	o
Timestamp	RFC 3261 [3]			o	o	o	o	o	o	o	o
To	RFC 3261 [3]	c (see note)	r	m	m	m	m	m	m	m	m
Unsupported	RFC 3261 [3]	420		-	m	-	m	m	m	m	o
User-Agent	RFC 3261 [3]			o	o	o	o	o	o	o	o
Via	RFC 3261 [3]	R	amr	m	m	m	m	m	m	m	m
Via	RFC 3261 [3]	rc	dr	m	m	m	m	m	m	m	m
Warning	RFC 3261 [3]	r		-	o	o	o	o	o	o	o
WWW-Authenticate	RFC 3261 [3]			-	-	-	-	-	-	-	-
P-Early-Media	RFC 5009 [29]	R	amr	-	-	-	o	-	o	o	-
P-Early-Media	RFC 5009 [29]	18x	amr	-	-	-	o	-	-	-	-
P-Early-Media	RFC 5009 [29]	2xx	amr	-	-	-	-	-	o	o	-
NOTE: Copied with possible addition of tag.											

6.3.5 SIP Bodies

SIP messages may, depending on the application and message type, contain one or more bodies to include information that is not encoded into SIP header fields.

This clause specifies the relevant body or content types to be supported by interface implementers.

The Session Description Protocol (RFC 4566 [6]) shall be used as specified further down in the present document.

Table 6.3 shows the SDP types, parameters and values that shall be supported for sending, receiving and processing.

Table 6.3: Supported SDP Types and Parameters

Description	SDP Types	SDP Parameters	Values
Session	Protocol version ("v=")	<SDP version number>	0
	Origin ("o=")	<username>	Values allowed in RFC 4566 [6]
		<sess-id>	Values allowed in RFC 4566 [6]
		<sess-version>	Values allowed in RFC 4566 [6]
		<nettype>	IN
		<addrtype>	IP4
		<unicast-address>	Values allowed in RFC 4566 [6]
	Session name ("s=")	<session name>	Values allowed in RFC 4566 [6]
	Connection data ("c=")	<nettype>	IN
		<addrtype>	IP4
		<connection-address>	Values allowed in RFC 4566 [6]
Time	Timing ("t=")	<start-time>	Values allowed in RFC 4566 [6]
		<stop-time>	Values allowed in RFC 4566 [6]
Media	Media descriptions ("m=")	<media>	audio
		<port>	(Application dependent)
		<proto>	RTP/AVP
		<fmt>	0 (for PCM-μ) 8 (for PCM-A) 101 (for DTMF), (see note)
	Attributes ("a=")	<send-receive mode>	recvonly sendrecv sendonly inactive
		rtpmap:<payload type> <encoding name>/<clock rate> (optional)	0 PCMU/8 000 (for PCM-μ) 8 PCMA/8 000 (for PCM-A) 101 telephone-event/8 000 (for DTMF)
		fmtp: (optional)	101, 0-15 (for DTMF)
NOTE: The payload types in the range 96 to 127 are dynamically assigned (RFC 3551 [i.19]). The value 101 which is used to define the telephone-event has to be seen as example out of the defined value range.			

6.3.6 SIP URI Convention

GSM-R networks and other telephony networks address their subscribers and route calls based on numeric addresses and numeric addressing schemes. EIRENE [1] specifies such an addressing scheme for GSM-R telephony. E.164 [23] specifies such an addressing scheme for public telephony networks.

In contrast, SIP User Agents are addressed and requests and responses are routed based on Uniform Resource Identifiers (RFC 3986 [25]). Various kinds of URIs can be routed in a SIP network.

At the present interface only SIP URIs shall be used in order to address Signalling Endpoints. These SIP URIs shall allow the addressing of EIRENE [1] as well as E.164 [23] numbers.

The generic augmented BNF [10] definition of a SIP URI can be found in RFC 3261 [3]. The following augmented BNF notation [10] specifies the SIP URI scheme that shall be implemented at the present interface:

SIP-URI = "sip:" user "@" host *(";" uri-parameter)

Where

user = eirene-user / e164user

eirene-user = 1*DIGIT

e164-user = "+" 1*DIGIT

host = hostname / IPv4addres

hostname = 1*(domainlabel ".") toplabel ["."]

domainlabel = alphanum *(alphanum / "-") alphanum

toplabel = 2*ALPHA

IPv4address = 1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT "." 1*3DIGIT

uri-parameter = user-param

user-param = "user=" ("phone" / "gsmr")

In addition to the above syntactical definition of the SIP URI scheme, the following clauses specify the semantics of this SIP URI scheme and how existing addressing schemes (i.e. EIRENE [1] and E.164 [23]) are incorporated into it.

6.3.6.1 Display Name

The display name is defined in RFC 3261 [3] as "not standardized optional text" preceding the SIP URI.

A display name may be used at the present interface, but it shall be ignored by all involved SIP entities.

6.3.6.2 User Part

The user part of the SIP URI at the present interface shall either contain:

- an international EIRENE [1] number if a GSM-R number is addressed; or
- an international E.164 [23] number consisting of a "+" and one or more digits if a PSTN, PLMN or PABX number is addressed.

6.3.6.3 Host Part

According to the above definition of the SIP URI scheme used at the present interface the host part is a fully qualified domain name or an IPv4 address as defined in [2].

RFC 3261 [3] defines an optional extension of the URI's host part with a service port. As this is not allowed at the present interface, the SIP service port defaults to 5 060.

The fully qualified domain name shall identify the subsystem (either NSS or FTS) that the addressed subscriber resides at.

At one logical NSS-FTS interface, exactly one fully qualified domain name shall be associated with the NSS and exactly one with the FTS.

In the SIP Contact header field the SIP URI's host part shall be provisioned with the Signalling Endpoint's IPv4 address since the subsystem's FQDN identifies the subsystem but not a specific Signalling Endpoint.

6.3.6.4 URI Parameters

The user parameter is mandatory within the SIP URI at the present interface.

The "user" parameter at the present interface shall either be set to:

- "gsmr" if an EIRENE GSM-R number is addressed; or
- "phone" if a PSTN, PLMN or PABX number is addressed (compare RFC 3261 [3], section 19.1.6).

All other SIP URI parameters specified by RFC 3261 [3] shall not be used.

6.3.6.5 Use

The specified SIP URI scheme shall be applied to the Request URI and the URIs in the following header fields:

- From;
- To;
- P-Asserted-Identity;

- Contact.

The general purpose and use of the From, To, and Contact header fields is defined in RFC 3261 [3] and fully applies to the present interface. The purpose and use of the P-Asserted-Identity header field, defined in RFC 3325 [13], is described in clauses 6.4.1 and 6.4.2 of the present document.

In order to enable a callee to call back the initiator of a session, within a single dialog, the content of all SIP URIs in the From, To, P-Asserted-Identity and Contact header fields shall be routable in the target network. It is the responsibility of the network operator to implement proper EIRENE [1] and E.164 [23] number routing in order to fully support the call-back capability within his private networks. As explained in clause 6.4.2 of the present document, the P-Asserted-Identity SIP URI shall have precedence over all other URIs for call-back.

The "user" parameter, as defined above, in conjunction with international numbers according to EIRENE [1] and E.164 [23], clearly indicates to which target network a call shall be routed. While it is still allowed and supported, this makes usage of breakout code routing (referred to as "call type 9" in EIRENE [1]) unnecessary.

Tables 6.4 and 6.5 show the required behaviour and illustrate the limitations (i.e. the allowed combinations) of SIP URIs in SIP requests and SIP responses at the present interface.

Table 6.4: Use of SIP URIs in Requests

Header Field	Request Target: EIRENE number		Request Target: E.164 number	
Request-URI	EIRENE SIP URI	EIRENE SIP URI	E.164 SIP URI	E.164 SIP URI
To	EIRENE SIP URI	EIRENE SIP URI	E.164 SIP URI	E.164 SIP URI
From	EIRENE SIP URI	E.164 SIP URI	EIRENE SIP URI	E.164 SIP URI
P-Asserted-Identity (note)	EIRENE SIP URI	E.164 SIP URI	EIRENE SIP URI	E.164 SIP URI
Contact	EIRENE SIP URI	E.164 SIP URI	EIRENE SIP URI	E.164 SIP URI
NOTE: The P-Asserted-Identity header field is only present when updated connected identity information is being transmitted. Therefore it is not be present in every request. See clause 6.4.2 of the present document for more information.				

Table 6.5: Use of SIP URIs in Responses

Header Field	Request Target: EIRENE number		Request Target: E.164 number	
Request-URI	n/a	n/a	n/a	n/a
To	EIRENE SIP URI	EIRENE SIP URI	E.164 SIP URI	E.164 SIP URI
From	EIRENE SIP URI	E.164 SIP URI	EIRENE SIP URI	E.164 SIP URI
P-Asserted-Identity (note)	EIRENE SIP URI	EIRENE SIP URI	E.164 SIP URI	E.164 SIP URI
Contact	EIRENE SIP URI	EIRENE SIP URI	E.164 SIP URI	E.164 SIP URI
NOTE: The P-Asserted-Identity header field is only present when updated connected identity information is being transmitted. Therefore it is not present in every response. See clause 6.4.2 of the present document for more information.				

6.3.6.6 Examples

This clause illustrates how common use cases map to valid SIP URI combinations at the present interface.

Table 6.6 shows an example where a GSM-R subscriber (049212345601) calls an FTS subscriber by its EIRENE functional number (04971234501).

Table 6.6: Use of SIP URIs - Example NSS to FTS

Header Field	Request	Response
Request-URI	sip:04971234501@fts.railway.com;user =gsmr	n/a
To	sip:04971234501@fts.railway.com;user =gsmr	sip:04971234501@fts.railway.com;user =gsmr
From	sip:049212345601@nss.railway.com;user =gsmr	sip:049212345601@nss.railway.com;user =gsmr
P-Asserted-Identity	not present	not present
Contact	sip:049212345601@10.0.0.1;user =gsmr	sip:04971234501@10.0.0.2;user =gsmr
NOTE 1: 049212345601 is the international EIRENE number of the calling GSM-R subscriber. NOTE 2: 04971234501 is the international EIRENE number of the called FTS subscriber.		

Table 6.7 shows an example where a PABX (accessible through and interconnected to the FTS) subscriber (+431811502222) calls a GSM-R subscriber by its EIRENE functional number (049212345601).

Table 6.7: Use of SIP URIs - Example PABX@FTS to NSS

Header Field	Request	Response
Request-URI	sip:049212345601@nss.railway.com;user =gsmr	n/a
To	sip:049212345601@nss.railway.com;user =gsmr	sip:049212345601@nss.railway.com;user =gsmr
From	sip:+431811502222@fts.railway.com;user =phone	sip:+431811502222@fts.railway.com;user =phone
P-Asserted-Identity	not present	not present
Contact	sip:+431811502222@10.0.0.2;user =phone	sip:049212345601@10.0.0.1;user =gsmr
NOTE 1: +43181150 is the international E.164 access number for the PABX. +431811502222 is the international E.164 number of the calling PABX subscriber. NOTE 2: 049212345601 is the international EIRENE number of the called GSM-R subscriber.		

Table 6.8 shows an example where a FTS subscriber (+4350005555) calls a PSTN subscriber (+4312345678) in a deployment scenario where the NSS provides PSTN access.

Table 6.8: Use of SIP URIs Example - FTS to PSTN@NSS

Header Field	Request	Response
Request-URI	sip: +4312345678@ nss.railway.com;user =phone	n/a
To	sip: +4312345678@ nss.railway.com;user =phone	sip: +4312345678@ nss.railway.com;user =phone
From	sip: +4350005555@fts.railway.com;user =phone	sip: +4350005555@fts.railway.com;user =phone
P-Asserted-Identity	not present	not present
Contact	sip: +4350005555@10.0.0.2;user =phone	sip: +4312345678@10.0.0.1;user =phone
NOTE 1: +4350005555 is an international E.164 number assigned to the FTS subscriber. NOTE 2: +4312345678 is an international E.164 public telephone number.		

6.3.7 Option Tags

Option tags are used to identify to SIP Endpoints the required, supported or unsupported SIP options/extensions. Table 6.9 lists the option tags which shall be used accordingly at the NSS-FTS interface by all SIP entities.

Table 6.9: Option tags

Option Tag	List in header field	Reference
100rel	Require, Supported	RFC 3262 [11]
privacy	Supported	RFC 3323 [15]
resource-priority	Require, Supported	RFC 4412 [12]
timer	Require, Supported	RFC 4028 [16]

6.4 Interface Functionality to Signalling Interface Mapping

This clause specifies in detail all signalling procedures required to support the functionalities described in clause 5. As the SIP signalling framework and well known SIP extensions provide solutions to the major part of the requirements, this is being done by referencing applicable RFCs. Deviations from and/or limited applicability of those RFCs are explicitly pointed out where appropriate.

6.4.1 Basic Call

This clause defines the signalling mechanisms applicable for basic call handling at the present interface.

The basic procedures for call setup, negotiation and establishment of an associated media session and call termination are defined in RFC 3261 [3] and RFC 3264 [4] and fully apply to the present interface. A successful example of these basic procedures is illustrated and explained in section 3.1 of RFC 3665 [i.9]. Sections 3.8, 3.9, 3.10 and 3.11 of RFC 3665 [i.9] show and explain some unsuccessful examples.

To increase the robustness of the interface and to enhance the support of interworking with circuit switched participants the PRACK method shall be used to reliably acknowledge all provisional responses at the present interface in accordance with RFC 3262 [11]. For this purpose all SIP Endpoints shall include the option tag 100rel (RFC 3262 [11]) in the Require header field of an INVITE request.

NOTE: As the PRACK method starts a new SIP transaction, the (final) response to the PRACK method may be sent after the final response to the initial INVITE. This means that the session establishment time is not considerably increased by this SIP extension.

Usage and purpose of the Request-URI, the From and the To header fields are defined and explained in RFC 3261 [3]. Clause 6.3.6 of the present document defines the SIP URI convention for the present interface and in particular specifies syntactically and semantically allowed SIP URIs in the Request-URI and the From, To, Contact and P-Asserted-Identity header field.

The Resource-Priority header field as specified in RFC 4412 [12] and in clause 6.4.5.1 in the present document shall be used for all INVITE requests between NSS and FTS to indicate the operational and resource priority of the call to the signalling partner. The resource-priority option tag, also defined in RFC 4412 [12], shall be listed in the Require header field in any INVITE request.

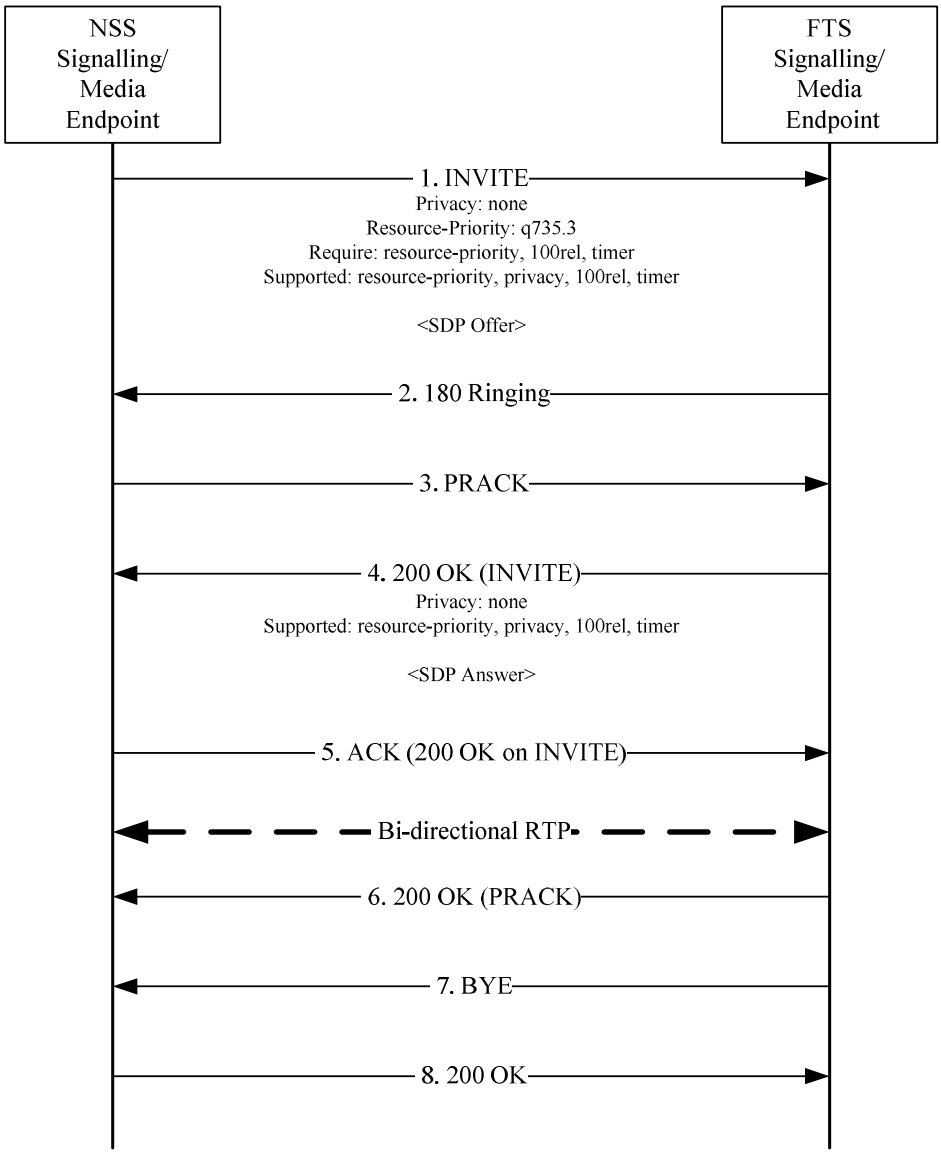
Although allowed and specified in RFC 3261 [3], SIP authentication/challenging shall not be performed at the present interface. See annex C of the present document.

At the present interface a dedicated SIP dialog shall be established for every call. Only two SIP UAs shall be involved in a SIP session's signalling flow, so that from the present interface's point of view there is exactly one SIP UA or Signalling Endpoint on either side of the interface. In case a call is to be delivered to several targets within the FTS/NSS subsystem the SIP UA exposed to the present interface shall act as a B2BUA as defined in RFC 3261 [3].

As mentioned and visualized in the reference architecture in clause 4 of the present document, the Signalling Endpoint and the Media Endpoint in each subsystem are different logical entities and may be different physical entities. Thus a SIP Endpoint always acts upon a Media Endpoint in the same subsystem that originates and/or terminates an RTP session. This is naturally the same in a SIP architecture as per RFC 3261 [3]. At the present interface Signalling Endpoints shall utilize the Session Description Protocol (SDP) described in RFC 4566 [6] according to the offer/answer model specified in RFC 3264 [4] to negotiate and set up a bi-directional, uni-cast media session, i.e. an RTP session.

RFC 3261 [3] defines two types of SDP offers: an "early" and a "late" offer. At the present interface only an "early" SDP offer shall be allowed, which is sent with a session's initial INVITE request.

Figure 6.1 illustrates a successful basic call scenario between two SIP Endpoints as specified in the present document. All interface specific header fields are shown.



NOTE: The Signalling and Media Endpoints are shown as one entity. This representation is used to enhance the readability of the diagrams and does not favour any physical implementation.

Figure 6.1: Successful session establishment and termination

At any time in the signalling flow, and for various reasons not specific to the present interface, such a basic call scenario may fail. Possible errors, possible reasons and how those errors shall be handled and indicated to the other signalling party is discussed in detail and explained in the RFCs referenced above.

6.4.2 Connected Parties Identity Information

SIP implicitly supports identity information exchange between connected parties with the header fields From and To as specified in RFC 3261 [3]. These header fields, mandatory in all requests and responses, contain URIs according to the SIP URI convention in clause 6.3.6 of the present document.

According to RFC 3261 [3] the identity information (URI) in the From and To header fields shall not be changed during a SIP dialog.

This restriction does not apply to the P-Asserted-Identity header field specified in RFC 3325 [13]. Therefore the P-Asserted-Identity header field shall be implemented at the present interface for the purpose of connected party identity updates in accordance with its specification in RFC 3325 [13] and RFC 5876 [14], as well as the content of this clause.

If, for any reason, a connected party identity changes an immediate identity information update shall be sent to the other party. Depending on the dialog state, such an identity update shall be sent with a final and positive response (200 OK) to an initial INVITE request or with a dedicated re-INVITE request, as defined in section 12 of RFC 3261 [3], if a dialog has already been established.

This means, that an update of identity information between the initial INVITE request and a final response to it is not possible at the present interface, as a re-INVITE shall not be sent in this dialog state as per RFC 3261 [3].

Furthermore, if a connected party identity differs from the content of the From header field when it is sending a SIP request or from the content of the To header field when it is sending a SIP response, it shall provide its current identity information to the respective other party using the P-Asserted-Identity header field in the same SIP request or response.

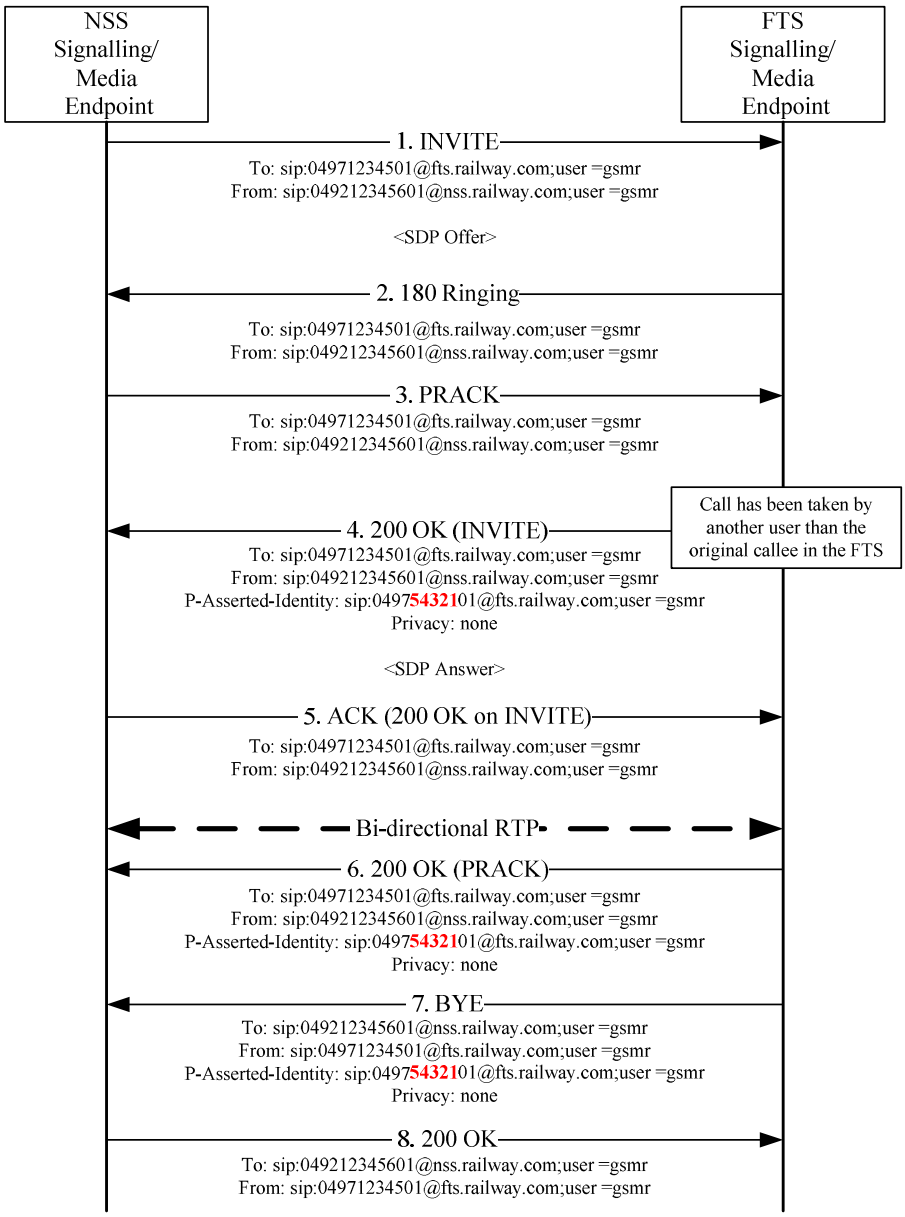
This means, if a connected party identity has changed within a SIP dialog, the content of the From and To header field remains unchanged, but the current identity information is provided in the P-Asserted-Identity header field to the other party in any SIP request or SIP response.

The SIP URI convention in clause 6.3.6 of the present document specifies valid content of the P-Asserted-Identity header field within the context of the present interface.

The Privacy header field, defined in RFC 3323 [15], shall be included in any request or response that contains a P-Asserted-Identity header field. The priv-value shall always be set to "none" at the present interface. This value avoids the removal of the P-Asserted-Identity header field by another SIP entity.

As the identity information provided in the P-Asserted-Identity header field is always the same as, or more up to date than, the From and To contained information, it has precedence over the information provided in the other header fields. Therefore the P-Asserted-Identity information shall be used for call-back.

Figure 6.2 shows the basic call scenario from figure 6.1 with the addition of an identity update, where the FTS sends back an updated identity with the 200 OK response to the initial INVITE. All header fields relevant to this feature are explicitly shown.



NOTE: The Signalling and Media Endpoints are shown as one entity. This representation is used to enhance the readability of the diagrams and does not favour any physical implementation.

Figure 6.2: Connected Party Identity Update

6.4.3 Media Session Renegotiation and Call Hold

Media session renegotiation using the re-INVITE method as defined in RFC 3261 [3] during an established dialog is allowed on the present interface and may be initiated by either side.

NSS and FTS SIP Endpoints which send changes to negotiated media capabilities via SIP re-INVITE shall support section 14 "Modifying an Existing Session" of RFC 3261 [3].

An NSS/FTS SIP Endpoint that participates in renegotiation shall be prepared to accept additional offers containing SDP with a version that has not changed, and shall generate a valid answer.

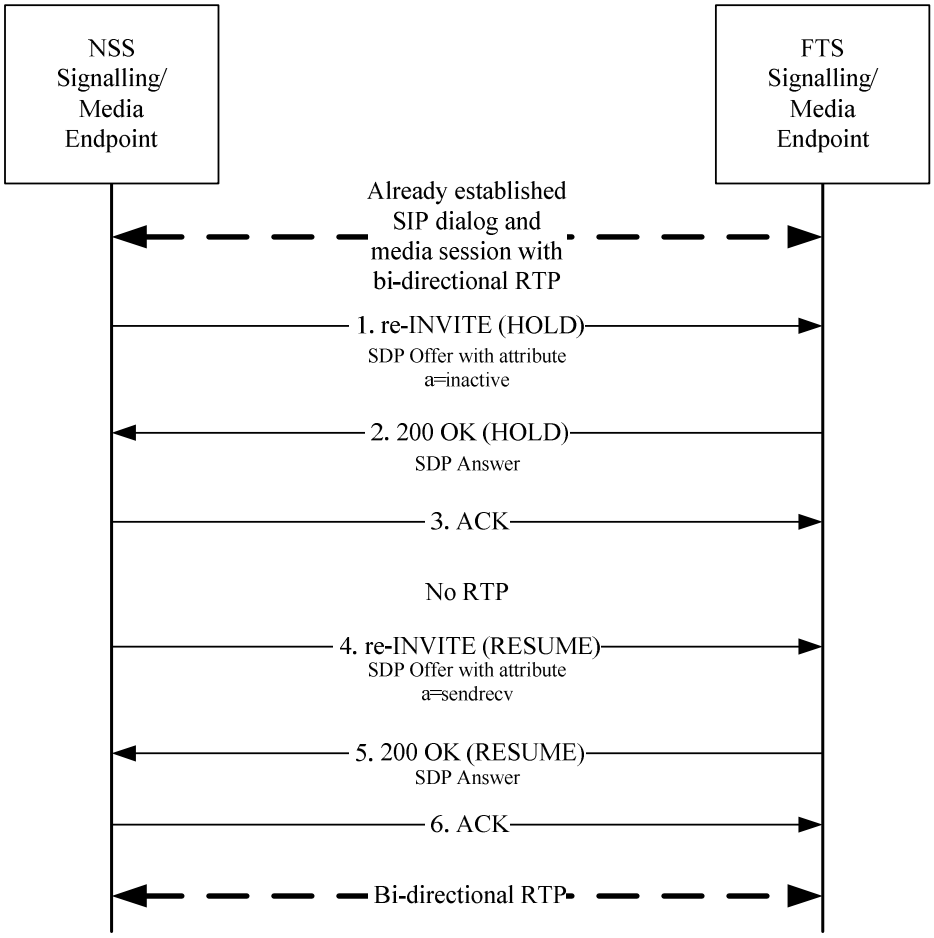
In SIP a special application of this media renegotiation mechanism is what is commonly referred to as Call Hold/Resume. RFC 4566 [6] defines the SDP attributes "recvonly", "sendrecv", "sendonly" and "inactive". At the present interface, these SDP attributes describe whether an RTP stream should be sent uni-directionally, bi-directionally or not sent at all. This SDP feature is commonly used to implement the Call Hold/Resume supplementary service in SIP/RTP environments.

At the present interface, if the NSS or FTS SIP Endpoint wants to put a media session on hold in an established dialog, a new SDP offer shall be sent with a re-INVITE request that contains:

- the "inactive" SDP attribute if the remote side should generate a hold tone; or
- the "sendonly" SDP attribute if an "On Hold Tone" or "Music On Hold" will be provided to the remote party from the initiating subsystem.

If the media session shall be resumed, a new SDP offer containing the "sendrecv" SDP attribute shall be sent in a new re-INVITE request.

Figure 6.3 illustrates such a scenario. All header fields relevant to this feature are explicitly shown.



NOTE: The Signalling and Media Endpoints are shown as one entity. This representation is used to enhance the readability of the diagrams and does not favour any physical implementation.

Figure 6.3: Call Hold/Resume Media Renegotiation

Another possible scenario is that the held session is transferred to another user within the NSS or FTS subsystem. This will lead to an update of the connected party and may also lead to an update of the attributes of the media session.

Figure 6.4 shows the corresponding message flow at the interface.

NOTE 1: How the session is transferred within the FTS is out of scope of the present document and is therefore not shown.

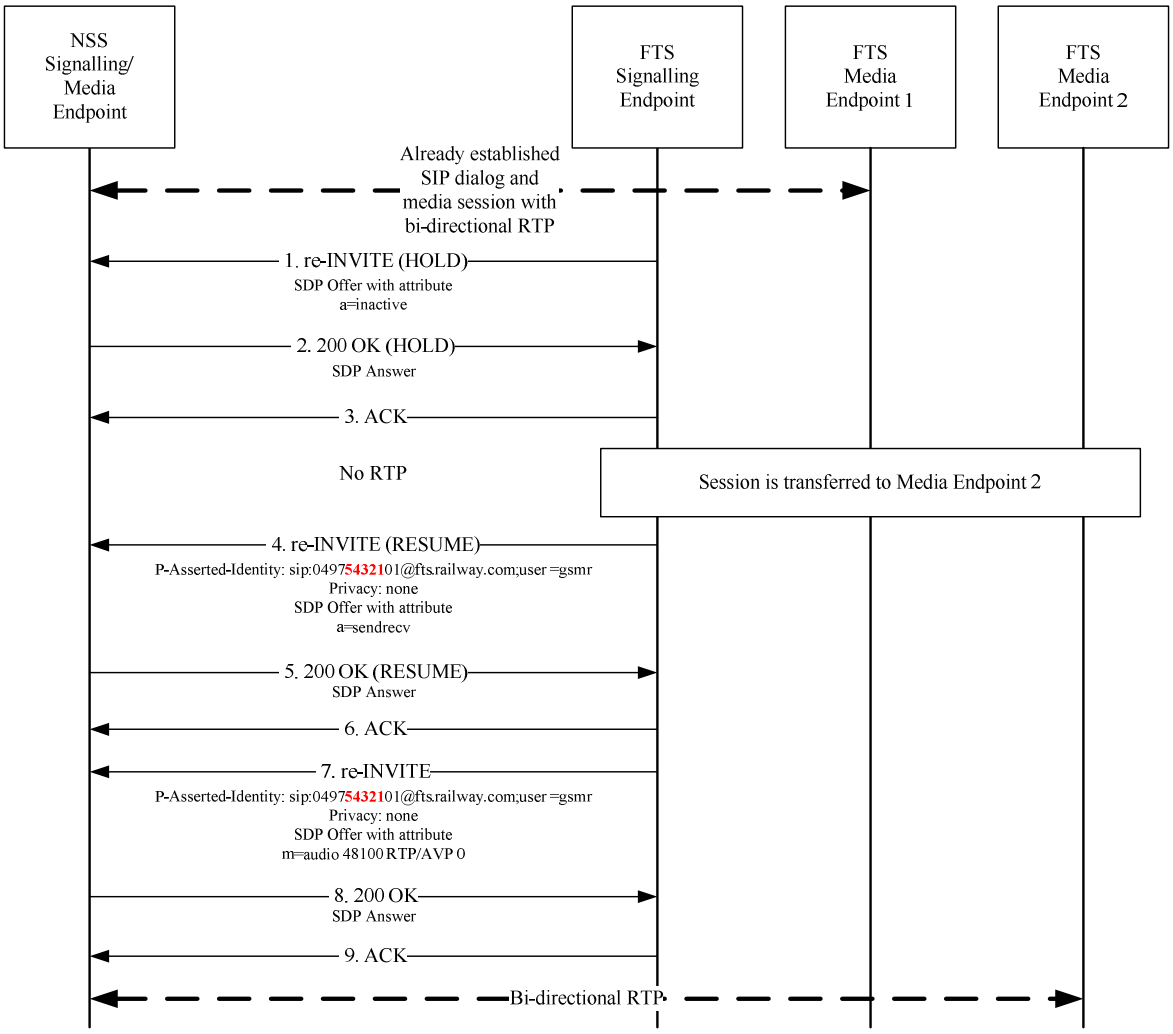


Figure 6.4: Identity and SDP Update after Session Transfer

NOTE 2: The Signalling and Media Endpoints are shown as one entity. This representation is used to enhance the readability of the diagrams and does not favour any physical implementation.

The existing session is put to hold (first re-INVITE) and then transferred to another user within the FTS (not shown here). The second re-INVITE (message number 4) resumes the session and provides the identity of the newly connected identity. The third re-INVITE (message number 7) is used for a new SDP offer, containing a new RTP endpoint in the example.

6.4.4 Early Media

Media exchange prior to final call acceptance or rejection is referred to as early media.

At the present interface only uni-directional, reverse early media shall be supported for the purpose of delivery of in-band announcements to a caller when available and required. It is the responsibility of the called subsystem, either NSS or FTS, to decide whether early media shall be provided.

RFC 3960 [i.10] discusses several issues with, and possible solutions for, early media in SIP. In particular potential issues with late SDP offers, parallel call forking and local tone generation are pointed out.

Clause 6.4.1 of the present document explicitly requires all SDP offers to be sent with the initial INVITE request. Thus the late SDP offer issue discussed in RFC 3960 [i.10] is not an issue at the present interface. Also clause 6.4.1 of the present document requires that only two SIP UAs are involved in a dialog establishment procedure. Thus call forking is not an issue with respect to early media at the present interface.

Additionally, the informational RFC 5009 [29] describes the P-Early-Media header, which can be used in SIP messages to request authorization of early media and to explicitly authorize early media using a direction parameter.

Regarding progress tone generation, a policy applicable to all SIP UAs at the present interface is defined in this clause, solving the local tone generation issue.

In the absence of early media the originating subsystem, FTS or NSS, shall generate and provide in-band progress indication tones to the user.

The originating subsystem may request explicit authorization of early media using the "supported" parameter in the P-Early-Media header in the initial INVITE.

Upon receipt of an early SDP answer or upon receipt of explicit authorization of early media with the direction parameter in the P-Early-Media header in a 18x response to the initial INVITE, the originating subsystem shall suppress local tone generation and shall instead present the media packets received to the user regardless of subsequent provisional responses like 180 Ringing that would trigger local tone generation. In such a case the called subsystem shall provide in-band progress tones if necessary.

The signalling flow for a call scenario with early media provision is almost the same as that of the basic call scenario.

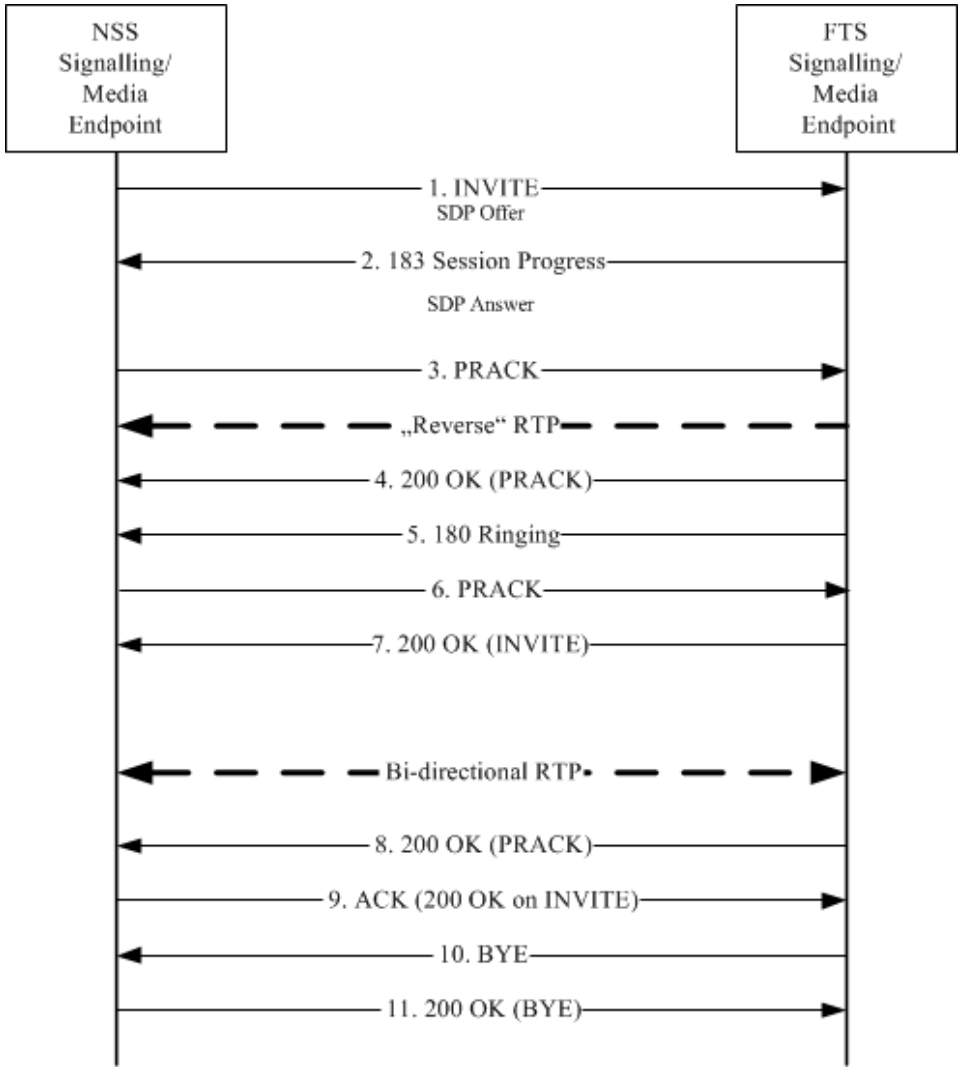
The callee may respond in the early dialog state to an INVITE request with a 183 Session Progress provisional response including an answer to the caller's SDP offer. It does not matter whether this is the first provisional response or not. Further provisional responses may be sent without an SDP answer. This SDP offer/answer shall be performed in accordance with RFC 3264 [4].

The 183 early media response shall be reliably acknowledged like any other provisional response at the present interface.

An early media session will either be transformed into a regular media session with the receipt of a final 200 OK response to the initial INVITE or will be terminated by negative final response.

Renegotiation of an early media session is not allowed at the present interface.

Figure 6.5 illustrates the signalling flow at the present interface for early media.



NOTE: The Signalling and Media Endpoints are shown as one entity. This representation is used to enhance the readability of the diagrams and does not favour any physical implementation.

Figure 6.5: Session establishment with early media and PRACK method

6.4.5 Multi Level Precedence and Pre-emption

The MLPP [24] service in EIRENE [1] and at the present interface is used to give precedence to higher priority calls over lower priority calls.

In order to ensure a deterministic quality of service a Signalling Endpoint at the present interface shall be able to either block further resource consumption by incoming lower priority calls or free resources for incoming higher priority calls. These actions shall be performed either in case of lack of resources or based on operational reasons.

Both NSS and FTS shall implement algorithms for detecting resource limits and also implement a local precedence and pre-emption policy. The local precedence and pre-emption policy shall define when and which calls are precedence blocked as well as when and which calls are pre-empted.

The specification of such algorithms and policies is out of scope of the present document and is subject to the NSS and FTS design.

In order to support the implementation of the MLPP service at the present interface, mechanisms for call priority flagging, release cause indication and signalling procedures for call precedence blocking and call and resource pre-emption are defined in this clause.

6.4.5.1 Resource Priority

The Resource-Priority header field as specified in RFC 4412 [12] shall be included in all INVITE requests between NSS and FTS to inform the partner about the operational and resource call priority. RFC 4412 [12] defines several resource priority namespaces. At the present interface the Q735 namespace shall be used. The Q735 namespace is chosen because it uses a pre-emption policy and a supporting Signalling Endpoint may disrupt an existing session to make room for a higher-priority incoming session. A Signalling Endpoint compliant with the present document shall terminate a session established with a lower-priority value in favour of a new session set up with a higher relative priority value, unless local policy has some form of call-waiting capability enabled. If a session is terminated, the BYE method is used with a 'Reason' header field indicating why the pre-emption took place.

The syntax, in augmented BNF notation [10], of the 'Resource-Priority' header field at the present interface is therefore:

Resource-Priority = "Resource-Priority" HCOLON r-value

r-value = namespace "." r-priority

namespace = "q735"

r-priority = "0" / "1" / "2" / "3" / "4"

The 'r-value' parameter indicates the request priority. These values shall correspond to precedence levels (MLPP priority), specified in [i.17], according to table 6.10.

Table 6.10: Mapping of Resource Priority to MLPP Priority

Resource-Priority	MLPP Priority
q735.0	0
q735.1	1
q735.2	2
q735.3	3
q735.4	4

The following example of the header field shows a GSM-R session with priority 0:

Resource-Priority: q735.0

All parts of RFC 4412 [12] other than the definition of the Resource-Priority header field are considered not applicable and therefore shall not be implemented at the present interface.

If the NSS or FTS receives an INVITE request without a Resource-Priority header field or with a Resource-Priority using a different namespace, the Signalling Endpoint at the present interface shall use the Resource-Priority q735.4 at the present interface.

6.4.5.2 Reason Indication for Precedence and Pre-emption Events

In case of a pre-emption or precedence event the partner of the dialog shall be informed about the reason why the call has been terminated. For this purpose the Reason Header Field in accordance with RFC 3326 [8] and described in clause 6.4.8 of the present document shall be used. The following reasons shall be supported.

If an existing session is pre-empted:

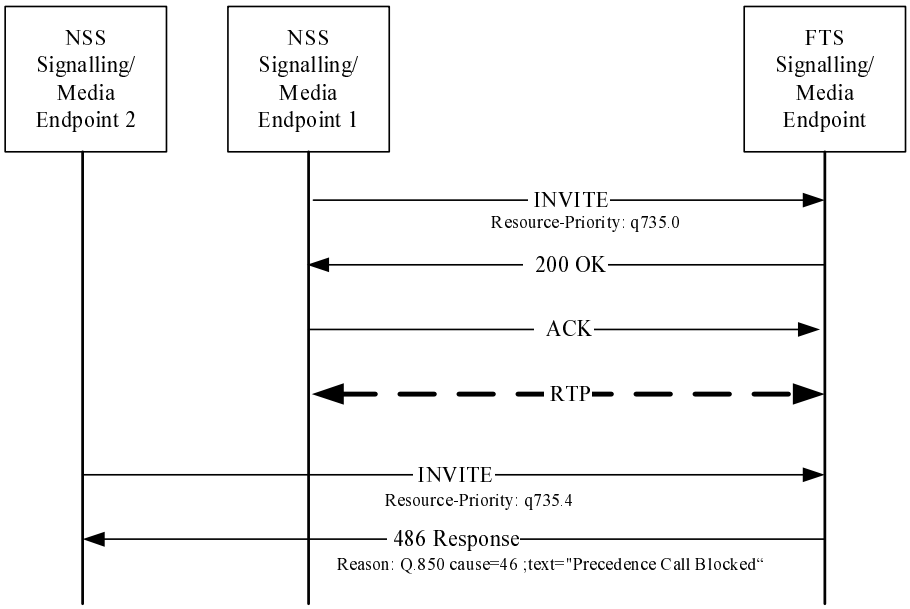
Reason: Q.850 ;cause=8 ;text="Preemption".

If a session could not be established because the called user is busy with sessions of equal or higher priority:

Reason: Q.850 ;cause=46 ;text="Precedence Call Blocked".

6.4.5.3 Signalling Procedure for Precedence Call Blocking

Figure 6.6 shows one example of the signalling procedure for precedence call blocking. There may be several other situations where call blocking is performed.

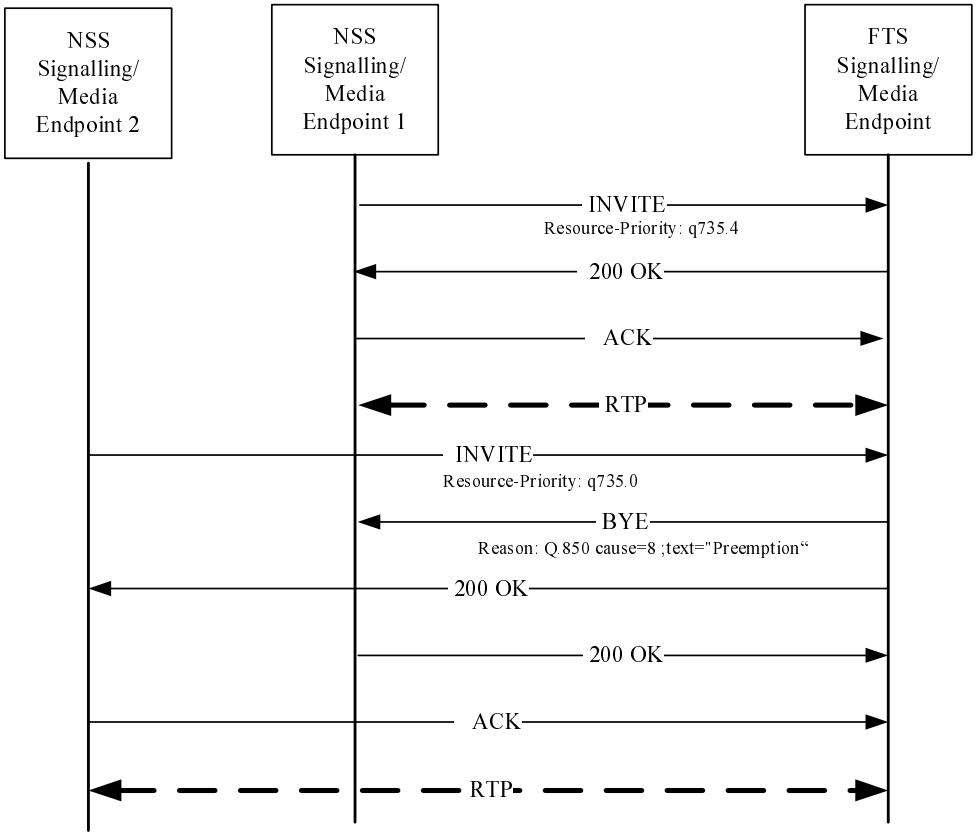


NOTE: The Signalling and Media Endpoints are shown as one entity. This representation is used to enhance the readability of the diagrams and does not favour any physical implementation.

Figure 6.6: Precedence Call Blocked

6.4.5.4 Signalling Procedure for Pre-emption

Figure 6.7 shows the signalling procedure for call pre-emption.



NOTE: The Signalling and Media Endpoints are shown as one entity. This representation is used to enhance the readability of the diagrams and does not favour any physical implementation.

Figure 6.7: Pre-emption of existing session

6.4.6 Group Call and Broadcast Call Control

Fixed Terminals shall use either DTMF tones to control VGCS/VBS calls at the present interface (as specified by EIRENE [1]) or explicit signalling on the Signalling Interface. DTMF handling at the present interface is specified in clause 7.4.1, explicit signalling is specified in clause 6.4.11.

Clause 7.4.1 and RFC 4733 [5] define reliability mechanisms to be implemented for DTMF events in the RTP stream. It is important to note that DTMF events may still get lost in case of heavy packet loss in the network.

Clause 6.4.11 defines a mechanism to implement explicit signalling on the Signalling Interface for Group Call and Broadcast Call control at the present interface. The handling of such explicit signalling within the endpoints of the present interface is out of scope of the present document.

The migration from DTMF tones to explicit signalling for Group Call and Broadcast Call control as well as the interworking of such control between NSS, implemented according to different 3GPP releases or architectures, is out of scope of the present document. However, for backwards compatibility reasons and in order to ensure interoperability, the usage of either DTMF tones or explicit signalling for Group Call and Broadcast Call control, as specified in the present document, shall be defined and agreed before the interconnection of the FTS and the NSS. Such an agreement shall be made on installation basis and not on call basis, i.e. a specific FTS shall apply the very same method for all calls.

6.4.7 User-to-User-Information-Element Transport

Following the approach of [i.1] a header field shall be used to transport the User-to-User information at the present interface.

If User-to-User information needs to be attached to call control messages at the present interface, the header field User-to-User, as specified in [i.1], but following the detailed specification below, shall be included in:

- INVITE requests;
- end-to-end responses to the INVITE requests; and
- BYE requests.

The following specification defines the User-to-User header field syntax using the augmented BNF notation [10]:

UUI = "User-to-User" HCOLON uui-data uui-param

uui-data = *33(HEXDIG HEXDIG)

uui-param = enc-param cont-param

enc-param = SEMI "encoding=hex"

cont-param = SEMI "content=gsmr-uui"

The first octet of the content shall be the protocol discriminator of the UUIE. The maximum length of the content (including the protocol discriminator) is limited to 33 octets to ensure transparency through all mobile and fixed elements of a GSM-R network. The content is carried in the uui-data field and encoded as defined in [9].

For example, the User-to-User header field of an INVITE request which transports the tag 5 (presentation of functional number [9]) would be:

User-to-User: 0005067370050005F1; encoding=hex; content=gsmr-uui.

The content is used to transport the functional number 370 750005 01.

6.4.8 Release Cause Transport

The Reason Header Field as specified in RFC 3326 [8] shall be used to transport Release Causes over the present interface. Such Release Causes are sent by the FTS or by the NSS in order to provide specific information about the reason for the release to GSM-R mobile terminals and Fixed Terminals.

Both protocols "SIP" and "Q.850" defined in RFC 3326 [8] shall be supported:

- When the protocol value "SIP" is used: The cause parameter contains a SIP status code.
- When the protocol value "Q.850" is used: The cause parameter contains a Recommendation ITU-T Q.850 [22] cause value in decimal representation.

The following example shows a possible usage:

Reason: Q.850 ;cause=16 ;text="Terminated".

6.4.9 SIP Session Timer

SIP [3] does not define a keepalive mechanism for the sessions it establishes. For instance, when a Signalling Endpoint fails to send a BYE message at the end of a session or the BYE message gets lost due to network problems, the other Signalling Endpoint or possibly a dialog stateful proxy will not know that the session has ended.

To resolve this problem the session timer as specified in RFC 4028 [16] shall be supported at the present interface.

Monitoring the RTP stream is not addressed by the SIP session timer. This functionality may be considered in a future release of the present document.

Signalling Endpoints send periodic re-INVITE or UPDATE requests (referred to as session refresh requests) to keep the session alive. The Signalling Endpoint which performs the initial request of the dialog, shall also perform the periodic refresh of the SIP session timer.

The interval for the session refresh requests is determined through a negotiation mechanism as described below. If a session refresh request is not received before the interval expires, the session is considered terminated. Both Signalling Endpoints are supposed to send a BYE, and any dialog stateful proxy can remove any state for the call.

Signalling Endpoints implementing the present interface shall issue periodic re-INVITE or UPDATE requests to keep the session alive. If the UAC and the UAS support the UPDATE method, it is recommended to use the UPDATE method to refresh the session.

The Session-Expires header field and the Min-SE header field as defined in RFC 4028 [16] shall be supported.

The minimum values for the MinSE and Session-Expires header fields should be pre-defined by the network operators so that about 90 % to 95 % of the operational calls should be finished before the session interval expires. The present document recommends the value of 600 seconds for both the Session-Expires and the Min-SE header field. Use of this fixed setting avoids unnecessary signalling traffic, otherwise, the negotiation of the session expiry timer would increase the dialog establishment time.

The initial INVITE request of a dialog shall include:

- the option tag 'timer' in the Supported header field;
- the Session-Expires header field with the pre-determined value and the refresher parameter set to 'uac';
- the Min-SE field with the pre-determined value.

If the UAC receives a 422 response message it shall retry the request. To avoid repeated negotiation of the Min-SE field for every INVITE request, the UAC may recognize the last accepted value, it has received and use it within its next request.

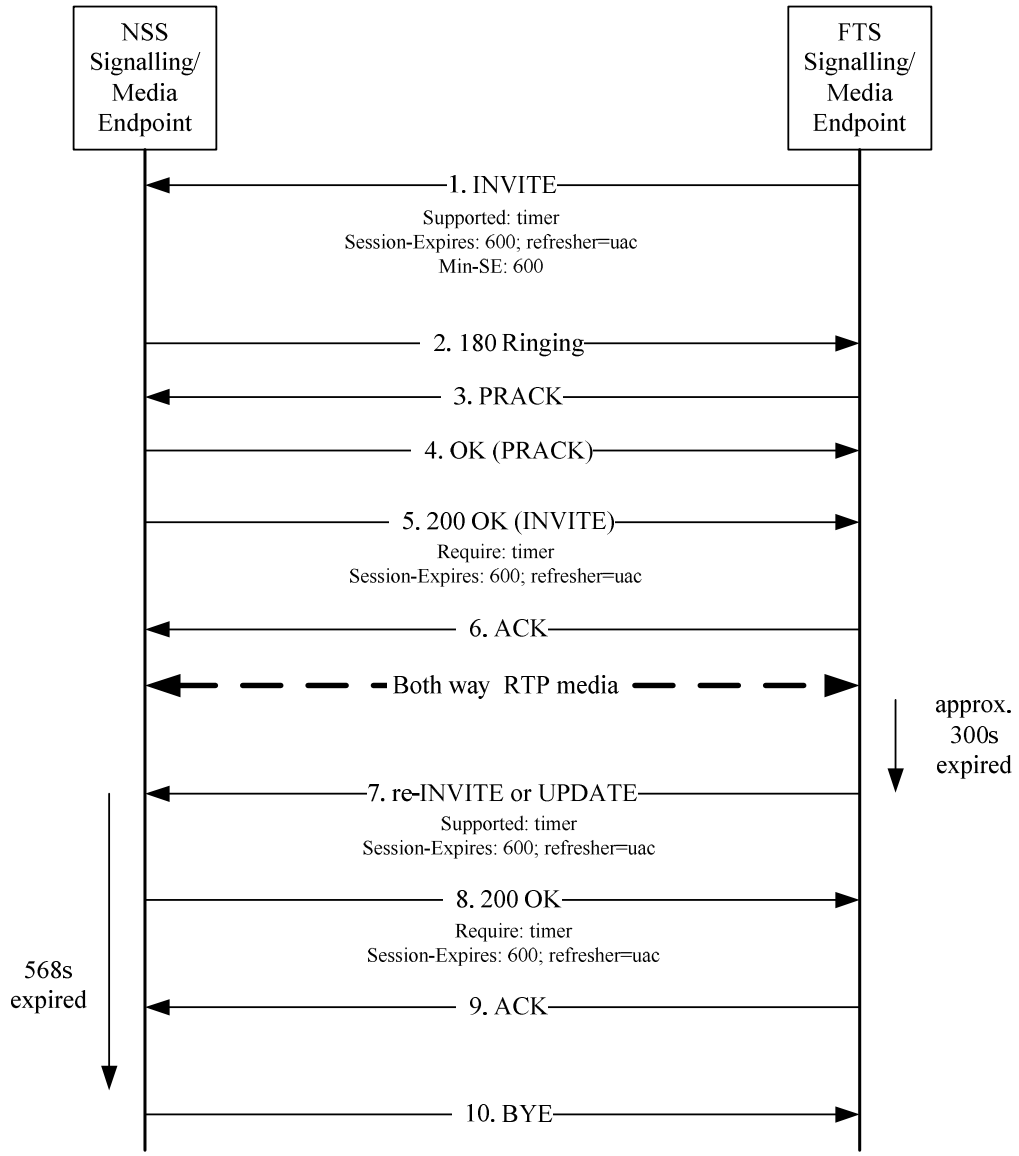
The Session-Expires header field shall be present in any re-INVITE or UPDATE sent within a dialogue with an active session timer, and its value shall be equal to the greater of the received Min-SE header field and the current session interval.

Preferably the role of the refresher does not change during an established dialog. Hence, the UAC initiating the request shall perform also the session refresh request and shall therefore set the refresher parameter to 'uac'.

A UAS receiving an initial session refresh request shall accept the refresher parameter in the Session-Expires header field and send back the same parameter value in the 2xx response. The UAS shall place a Require header field into the response with the value 'timer'.

Figure 6.8 shows an example signalling flow. The UAC, located within the FTS, requests a session timer refresh every 600 seconds. Because the Session-Expires equals the pre-determined value, the UAS accepts the value within the 200 OK response.

The UAC, as refresher, therefore sends a re-INVITE or UPDATE request approximately 300 seconds later to refresh the session. Shortly afterwards, the UAC crashes and does not send any further session refresh requests. Approximately 568 seconds later (600-32 as per recommendation in RFC 4028 [16]) the UAS times out and sends a BYE request.



NOTE: The Signalling and Media Endpoints are shown as one entity. This representation is used to enhance the readability of the diagrams and does not favour any physical implementation.

Figure 6.8: Example Session Timer Flow

6.4.10 OPTIONS Processing

The SIP OPTIONS method allows SIP peers to query each other for capabilities. The syntax of the OPTIONS message is described in RFC 3261 [3].

The OPTIONS message shall be transmitted directly to the SIP peer and not to an intermediary SIP entity and shall address a SIP peer using a SIP URI according to the following augmented BNF notation [10]:

SIP-URI = "sip" HCOLON hostport"

hostport = host

host = hostname / IPv4Address

IPv4Address = 1*3DIGIT "." 1*3DIGIT "."1*3DIGIT "."1*3DIGIT

For the definition of hostname see clause 6.3.6 of the present document.

Although sending of OPTIONS requests is an optional feature of SIP entities at the present interface, processing and replying to OPTIONS requests is a mandatory feature.

A SIP entity that receives an OPTIONS message shall respond with a status code indicative of its present ability to process SIP signalling messages.

A SIP entity shall respond to an OPTIONS method with a 200 response code when it is able to process SIP messages, unless the following response code is more appropriate.

When a replying SIP entity is currently unable to process additional SIP messages, it should respond with a 503 response code. A 503 response code should also used when a SIP entity is placed into a maintenance mode to indicate that it cannot accept new SIP dialogs. A replying SIP entity may include a Retry-After header in a response to the OPTIONS message to avoid further requests for a desired period of time.

To avoid unduly taxing a receiving SIP entity, transmitters of OPTIONS messages shall honour the Retry-After header field, if received.

6.4.10.1 OPTIONS Heartbeating

To enhance the efficiency and robustness of the present interface, the SIP Endpoints should have knowledge of the status of their partner entities. To prevent unnecessary delay due to timeouts and subsequent message re-transmissions, a method by which each entity may discover the operational status of its communicating peers is defined in this clause. Whereas the SIP Session timer (clause 6.4.9) is used to monitor already established dialogs, the OPTIONS heartbeating is used to regularly verify the availability of and the connectivity to partner entities (either Signalling Endpoints or proxy servers) of the partner subsystem.

The present document proposes the use of the OPTIONS method to determine the operational status of partner entities. The implementation of this heartbeating mechanism is optional. If a heartbeating mechanism is supported, the following behaviour shall be mandatory.

A SIP entity may transmit an OPTIONS message outside of a dialog at any desired interval in order to determine the status of another SIP entity. The transmitting and receiving SIP entities may be SIP User Agents or SIP proxy servers.

Any two entities that communicate with each other on a regular basis may be configured to transmit an OPTIONS message from time to time as provisioned by the network operator. It is recommended to exchange OPTIONS messages only when no other traffic is active.

If the sender of the OPTIONS message does not receive a response from its partner entity, there is no direct consequence to the behaviour of the sender. Especially, if there are dialogs or sessions in progress, their state shall not be changed. It is recommended that the sender notices the fact and uses other partner entities for establishing dialogs until an answer to the OPTIONS message is received. The detailed behaviour of the entity in such a case is subject to the NSS/FTS design and implementation and out of scope of the present document.

6.4.11 Signalling for Group Call and Broadcast Call Control

The SIP INFO and SIP BYE methods shall be utilized to control group calls and broadcast calls. The SIP INFO method shall be used to send mute or un-mute commands, where-as the BYE method shall be used if the group call shall be terminated.

Table 6.11 shows the extensions of the SIP message body with specific add-ons to exchange the group call and broadcast control commands.

Table 6.11: SIP message body extension for group call and broadcast call control

Method	Parameter	Value(s)	
VGCS-Control	action	kill, mute, unmute	mandatory
	sequence	DTMF digits	optional
	tone-length	DTMF tone length	optional
	tone-pause	DTMF tone pause	optional

Table 6.12 shows the specific parameters of the extensions of the SIP message body for group call and broadcast call control.

Table 6.12: SIP message body parameters for group call and broadcast call control

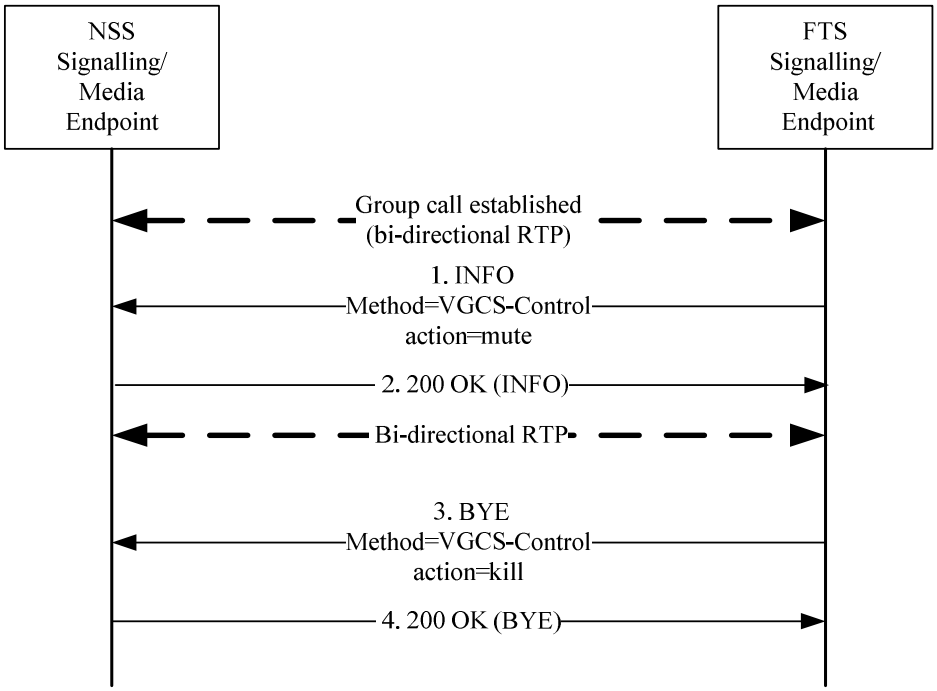
Parameter	Value(s)	Description
Action	"kill"/"mute"/"unmute"	This parameter describes the action, which is requested to be performed.
sequence	"***"/"###"/"#**"	This value defines the tone sequence to be sent to the group call register.
tone-length	*DIGIT	The value defines duration in ms of a single DTMF tone of the sequence.
tone-pause	*DIGIT	The value defines pause in ms between two DTMF tones of the sequence.

The parameters sequence, tone-length and tone pause are optional. They shall be sent if the parameters sequence, tone-length and tone-pause differ from the values defined in [EIRENE SRS] and for backwards-compatibility.

EXAMPLE: SIP INFO message transporting a mute sequence.

```
Session Initiation Protocol
    Request-Line: INFO sip:0495012345579@nss.railway.com;user=gsmr SIP/2.0
    Message Header
        …
        Info-Package: etsi.groupcall.control
        …
    Message Body
        Line-based text data: text/plain
            Method=VGCS-Control\r\n
            action=mute\r\n
            sequence=###\r\n
            tone-length=70\r\n
            tone-pause=65\r\n
```

Figure 6.9 illustrates the signalling flow to control a group call at the present interface. The establishment of the voice group call is not shown.



NOTE: The Signalling and Media Endpoints are shown as one entity. This representation is used to enhance the readability of the diagrams and does not favour any physical implementation.

Figure 6.9: Signalling for Group Call and Broadcast Call control

If a controller requests to talk, the FTS shall send a SIP INFO method with the Method=VGCS-Control and action "mute" to mute the uplink at the radio interface.

If the FTS terminates the voice group call, it shall send a SIP BYE method with the Method=VGCS-Control and action "kill".

If the SIP INFO method is used to send control info for group calls or broadcast calls, then the INFO request shall contain an *Info-Package* header according to RFC 6086 [i.3], containing the info package name *etsi.groupcall.control*. If the info package is not supported by the receiver, then the receiver shall reject the INFO request with 469 Bad Info Package according to RFC 6086 [i.3].

It is strongly recommended UAs on both ends of the present interface should utilize the *Recv-Info* header according to RFC 6086 [i.3], in order to indicate their willingness to support info package *etsi.groupcall.control*.

EXAMPLE: Indicating willingness to support info package in SIP INVITE message.

```
Session Initiation Protocol
    Request-Line: INVITE sip:0495012345579@nss.railway.com;user=gsmr SIP/2.0
    Message Header
        …
        Recv-Info: etsi.groupcall.control
        …
    Message Body
```

7 Media Interface

7.1 Network Layer Protocol

NSS and FTS shall use IPv4 [2] as the network layer protocol.

Network Address Translation (NAT) is a method used for IP address translation between address realms. NAT adds complexity to higher layer protocols that is not dealt with in the present document. Therefore no form of NAT shall be implemented in the network infrastructure at the media interface. See [i.16] for more information on NAT.

7.2 Transport Layer Protocol

NSS and FTS shall use UDP [26] as the transport layer protocol.

Network Address and Port Translation (NAPT) is a form of NAT that extends to the OSI transport layer. For the same reason as for pure network layer NAT, NAPT shall not be implemented in the network infrastructure at the media interface. See [i.16] for more information on NAPT. Any Media Endpoint that originates and/or terminates RTP traffic over UDP shall use the same UDP port for sending and receiving session media. This behaviour is referred to as symmetric RTP.

7.3 Real-Time Transport Protocol

A Media Endpoint shall transport and receive voice samples and telephony events using the real-time transport protocol (RTP) as described in RFC 3550 [7].

At the present interface only uni-cast RTP streams shall be supported.

7.3.1 Media inactivity detection

At the present interface the reception of RTP packets is supervised. For this purpose, a media inactivity timer shall be used. If no RTP packets are received for an established session the media inactivity timer shall be started. The media inactivity timer shall be reset if RTP packets are received again for an established session.

If the media inactivity timer expires, the Signalling Endpoint shall be informed that this timer is expired and the Signalling Endpoint shall release the corresponding SIP dialog.

The media inactivity timer shall be activated as soon as the media session is established between the Media Endpoints.

The media inactivity timer shall only be activated, when the media session is established with the SDP attributes "sendrecv" or "sendonly".

The value of the media inactivity timer shall be implementation specific and is therefore out of scope of the present document.

7.4 Media Codecs

Recommendation ITU-T G.711 [27] µ-Law and A-Law PCM codecs with a packetization rate of 20 ms shall be supported between the Media Endpoints at the present interface as shown in table 7.1. Additional packetization rates may be negotiated by SDP offer/answer model.

Table 7.1: Media codecs and recommended packetization rates

Codec	Support	Proposed packet size [ms]
G.711a	Mandatory	20
G.711µ	Mandatory	20

7.4.1 DTMF

DTMF as specified in RFC 4733 [5] shall be supported at the present interface. Each Media Endpoint shall use the procedures according to RFC 4733 [5] to transmit DTMF tones using the RTP telephone-event payload format. NSS and FTS Signalling Endpoints shall advertise support for receiving DTMF in every SDP offer/answer procedure. In-band (audio) transmission of DTMF is not allowed at the present interface.

The supported DTMF-related event codes within the telephone-event payload format are defined in table 7.2.

Table 7.2: DTMF named Events

Event	Code	Type	Volume?
0 to 9	0 - 9	tone	yes
*	10	tone	yes
#	11	tone	yes
A - D	12 - 15	tone	yes

The supported events shall be included in an "a=fmtp:" line as described in [5].

To provide backwards compatibility with implementations following RFC 2833 [28], even if the SDP data does not have an associated "a=fmtp:" line, both NSS and FTS Endpoints shall be prepared to receive telephone-event packets for all events in the range 0 to 15 and both entities shall be prepared to accept SDP with a payload type mapped to telephone-event.

At the present interface both reliability mechanisms defined in section 2.6.2 of RFC 4733 [5] shall be implemented to reduce the impact of packet loss on DTMF events.

7.4.1.1 Limitations to RFC 4733

Section 4 of RFC 4733 [5] shall not be supported at the present interface.

Packing multiple events into one packet, as described in section 2.5.1.5 of RFC 4733 [5] shall not be performed at the present interface.

SRTP is not supported at the present interface at all, hence its use for DTMF as mentioned in section 6 of RFC 4733 [5] is not supported either.

8 Recorder Interface

8.1 Reference Architecture

The system architecture used to identify the interface that is the subject of this clause is a simplification of a GSM-R Recording system down to a minimum of logical entities relevant to the present document.

Within this context the GSM-R recording system is logically divided into a GSM-R network and a Recorder Subsystem. The interface between the Mobile Terminals and the NSS as well as the interface between the Fixed Terminals and the FTS are explicitly not addressed in the present document. The focus of this clause is solely:

- the Signalling Interface; and
- the Media Interface;

between the logical subsystem SRS (Session Recording Server) and the logical subsystem SRC (Session Recording Client).

Figure 8.1 illustrates the reference system architecture.

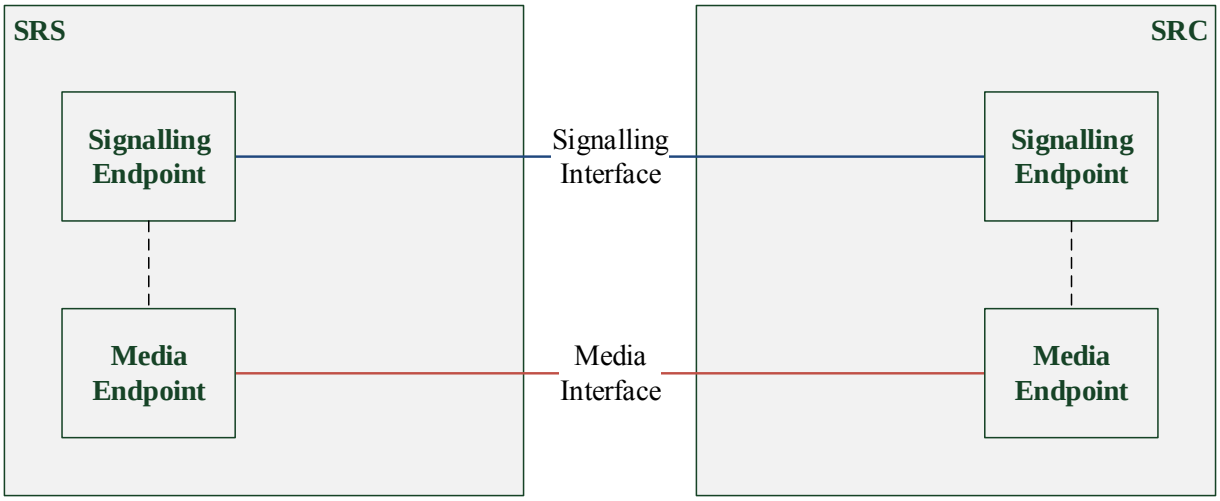


Figure 8.1: Reference Architecture (Recording)

One Signalling Endpoint maintains a Recording Session (RS) that is a SIP session created between SRC and SRS for the purpose of recording a Communication Session (CS). A CS represents a session that is the subject of recording.

One Signalling Endpoint may establish more than one RS and one Media Endpoint may be involved in one or more RS.

The Media Endpoint(s) are controlled by (a) Signalling Endpoint(s) in the same subsystem. This control mechanism is out of scope of the present document.

The maximum number of Signalling Endpoints allowed to be involved in a single call on the present interface is two - one on each side.

Optionally deployed Signalling Proxies may be involved in the signalling flow for either incoming traffic or outgoing traffic or both incoming and outgoing traffic at either side of the interface, as described in clause 4 of the present document.

8.2 Interface Functionality

This clause specifies functional requirements of the interface. The technical details are specified in clauses 8.3, 8.4 and 7 of the present document.

8.2.1 Recording Session

The primary function to be delivered by the present interface is the means to initiate and tear down a simplex audio (voice) connection between the SRS and SRC with a single, logical, SIP Endpoint involved per connection on each side of the present interface that controls the connection as well as its respective Media Endpoint (compare clause 8.1).

Such a connection (RS) is initialized by the SRC. The initiation phase shall specifically provide means and mechanisms for per recording session capability exchange, media negotiation, as well as error indication and handling.

A RS is a SIP session with specific extensions applied, and these extensions are listed in the procedures for SRC and SRS in clause 8.3. When an SRS receives a SIP session that is not a recording session, it is up to the SRS to determine what to do with the SIP session. Clause 7 and 8.4 provide recommendations and guidelines for RTP in the context of an RS.

8.3 Signalling Interface

The SRC initiates a recording session by sending a SIP INVITE request to the SRS. The SRC and the SRS are identified in the From and To headers, respectively.

Table 8.1 shows the changes to table 6.1 which shall be supported on the SRS/SRC interface.

Table 8.1: Changes to table 6.2 (SIP Header Fields)

Header field	Reference	Where	Proxy	ACK	BYE	CAN	INV	OPT	PRA	UPD	INF
Call-Info	RFC 3261 [3]		ar	-	-	-	m	o	-	o	o

Table 8.2 shows the changes to table 6.2 which shall be supported on the SRS/SRC interface.

Table 8.2: Changes to table 6.3 (supported SDP Types and Parameters)

Description	SDP Types	SDP Parameters	Values
Media	Attributes ("a=")	label: (optional)	(Application dependent)

Table 8.3 shows the changes to table 6.9 which shall be supported on the SRS/SRC interface.

Table 8.3: Changes to table 6.9 (option tags)

Option Tag	List in header field	Reference
siprec	Require, Supported	Internet-Draft [i.20]

A feature parameter describes a feature of a SIP Endpoint associated with the URI in the Contact header field. Table 8.4 lists feature parameters which shall be used accordingly at the SRS/SRC interface by all SIP entities.

Table 8.4: Feature Parameter

Feature Parameter	List in header field	Reference
+sip.src	Contact	RFC 3840 [30]
+sip.srs	Contact	RFC 3840 [30]

The SRC shall include a Resource-Priority header as specified in clause 6.5.4.1 and as shown in table 6.1 in each INIVITE request sent to the SRS containing the resource priority of the CS. This is to inform the SRS about the resource priority of the CS and requires no specific action related to the header field at the SRS.

The SRC shall include the '+sip.src' feature tag in the Contact URI for all recording sessions. An SRS uses the presence of the '+sip.src' feature tag in dialog creating and modifying requests and responses to confirm that the dialog being created is for the purpose of a RS.

An SRC shall include the 'siprec' option tag in the Require header when initiating a Recording Session so that SIP Endpoints which do not support this extension will simply reject the INVITE request with a '420 Bad Extension'.

When an SRS receives a new INVITE, the SRS shall only consider the SIP session as RS when both the '+sip.srs' feature tag and 'siprec' option tag are included in the INVITE request.

The INVITE request sent from the SRC shall contain a Call-Info header including a service-URN providing a unique communication session identifier and a reference to the m-line represented by a label (equal to labels within the RS SDP as in RFC 4574 [31]) with the header parameter 'purpose=etsi-csid'. In addition the same header shall include a reference to a meta data repository (URL) with the header parameter 'purpose=info.'

SRC and SRS should implement HTTP as the reference interface for metadata, but may be capable of fall-back to FTP.

NOTE: The data structure for meta data is out of scope of the present document. Required attributes, syntax and semantic are usually agreed on a bilateral level.

The service-URN shall include both, CS identifier and label according to the following augmented BNF notation [10]:

service-URN = "urn:etsi:csid:" csid

csid = identifier "." label

identifier = let-dig

label = dig

let-dig = ALPHA

dig = DIGIT

ALPHA = %x41-5A / %x61-7A ; A-Z / a-z

DIGIT = %x30-39 ; 0-9

Combining label and CS identifier helps to uniquely identify streams corresponding to a CS that are part of a single RS.

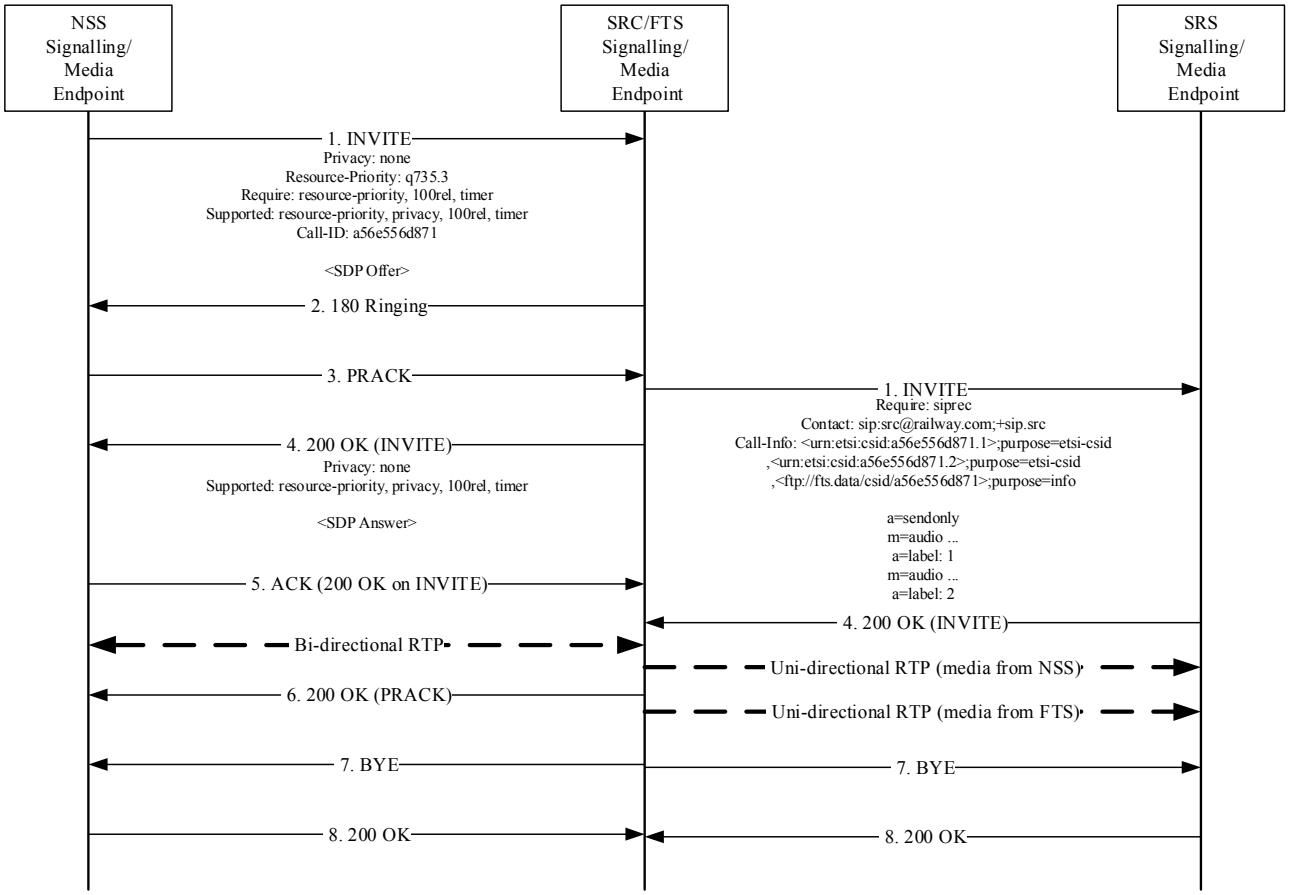
EXAMPLE 1: SIP INVITE initiating an RS that refers to a CS (identifier: a56e556d871) with two corresponding RS streams (label: 1,2) and a reference to a meta data repository via http.

```
Session Initiation Protocol
    Request-Line: INVITE sip:srs@railway.com SIP/2.0
    Message Header
        …
        Require: siprec
        Contact: sip:src@railway.com;+sip.src
        Call-Info: <urn:etsi:csid:a56e556d871.1>;purpose=etsi-csid
        ,<urn:etsi:csid:a56e556d871.2>;purpose=etsi-csid
        ,<http://fts.data/csid/a56e556d871>;purpose=info
        …
    Message Body
        …
        m=…
        a=label: 1
        m=…
        a=label: 2
```

EXAMPLE 2: SIP INVITE initiating an RS that refers to three individual CS (identifier: a56e556d871, a56e556d123, a56e556c9h1) with corresponding RS streams (label: 1,2,3) and a reference to a meta data repository via ftp.

```
Session Initiation Protocol
    Request-Line: INVITE sip:srs@railway.com SIP/2.0
    Message Header
        …
        Require: siprec
        Contact: sip:src@railway.com;+sip.src
        Call-Info: <urn:etsi:csid:a56e556d871.1>;purpose=etsi-csid
        ,<urn:etsi:csid:a56e556d123.2>;purpose=etsi-csid
        ,<urn:etsi:csid:a56e556c9h1.3>;purpose=etsi-csid
        ,<ftp://fts.data/csid/a56e346d221>;purpose=info
        …
    Message Body
        …
        m=…
        a=label: 1
        m=…
        a=label: 2
        m=…
        a=label: 3
```

Figure 8.1 illustrates the signalling flow to record media from NSS and FTS with FTS acting as SRC. The FTS forwards media in separate streams – one received from the NSS (label: 1) and one sent to the NSS (label: 2).



NOTE: The Signalling and Media Endpoints are shown as one entity. This representation is used to enhance the readability of the diagrams and does not favour any physical implementation. Only header field relevant to the recording function are shown.

Figure 8.2: Signalling for Basic Call and Recording

8.4 Media interface

This clause specifies media interface capabilities in addition to clause 7.

8.4.1 Media mxing

When using mixing, the SRC combines RTP streams from different participants and sends them towards the SRS using its own SSRC.

The SSRCs from the contributing participants shall be conveyed as CSRCs identifiers. The SRC includes one m-line and a unique label for each RTP session in an SDP offer to the SRS.

Having received the answer, the SRC shall start sending media to the SRS as indicated in the answer.

8.4.2 Multiple streams

When using multiple streams (m-lines), an SRC includes each m-line (unique label per m-line) in an SDP offer to the SRS.

Having received the answer, the SRC shall start sending media to the SRS as indicated in the answer or if the SRC deems the level of support indicated in the answer to be unacceptable, it may initiate another SDP offer/answer exchange in which an alternative RTP session (refer to clause 8.4.1) usage is negotiated.

Annex A (normative): Locating SIP Entities

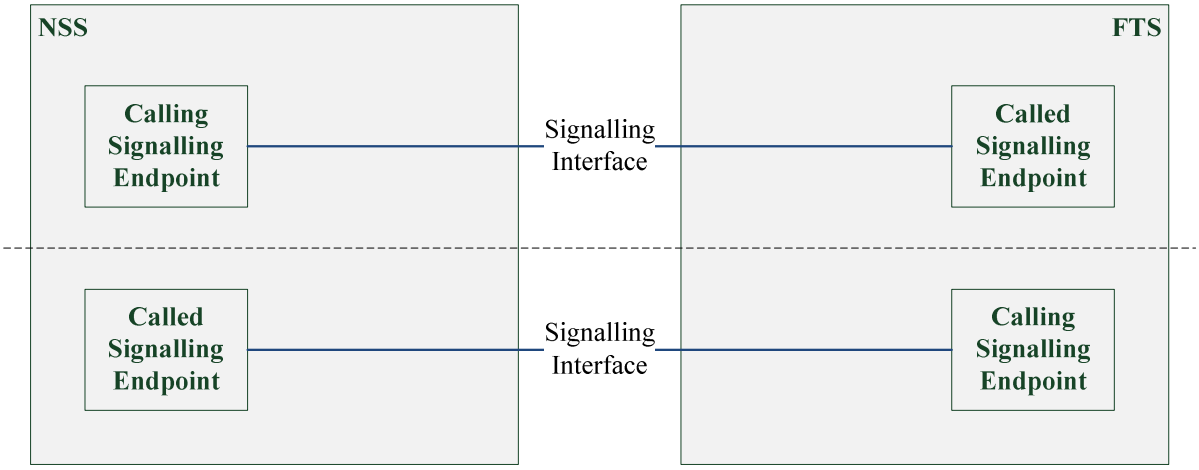
RFC 3263 [i.13] specifies a sophisticated framework to locate SIP servers in a SIP network, addressing a great variety of discovery and location issues in SIP networks.

Clause 4 of the present document explains and defines the reference system architecture and identifies logical SIP entities at the present interface. As the SIP network design and its complexity at the present interface is fairly simple, a simplified approach for locating SIP entities compared to RFC 3263 [i.13] is defined in this annex. In particular it defines how to locate a target SIP entity for an outgoing call by the means of its IP address.

Clause 6.3.6 of the present document defines a SIP URI convention for the signalling interface. Of special interest with respect to SIP entity location is the definition of the hostpart: One fully qualified domain name shall be used to address the FTS and another one to address the NSS. In other words, all outgoing traffic from one subsystem will have the same FQDN in its Request-URI's hostpart. No information reflecting the target subsystem's specific architecture or any deployment specifics is available or allowed in a SIP URI at the present interface.

Hence, the FQDN in the Request-URI's hostpart shall point to all SIP entities at which the receiving subsystem expects or is set up to receive incoming traffic. This may either be any number of SIP proxies, if the receiving subsystem consists of SIP proxies and SIP Endpoints and wants incoming traffic to pass via its SIP proxies, or any number of SIP Endpoints, if the target subsystem does not require incoming traffic to pass through its SIP proxy/proxies or if the target subsystem does not include any SIP proxies at all. The following figures show several deployment scenarios and their meaning with respect to this annex.

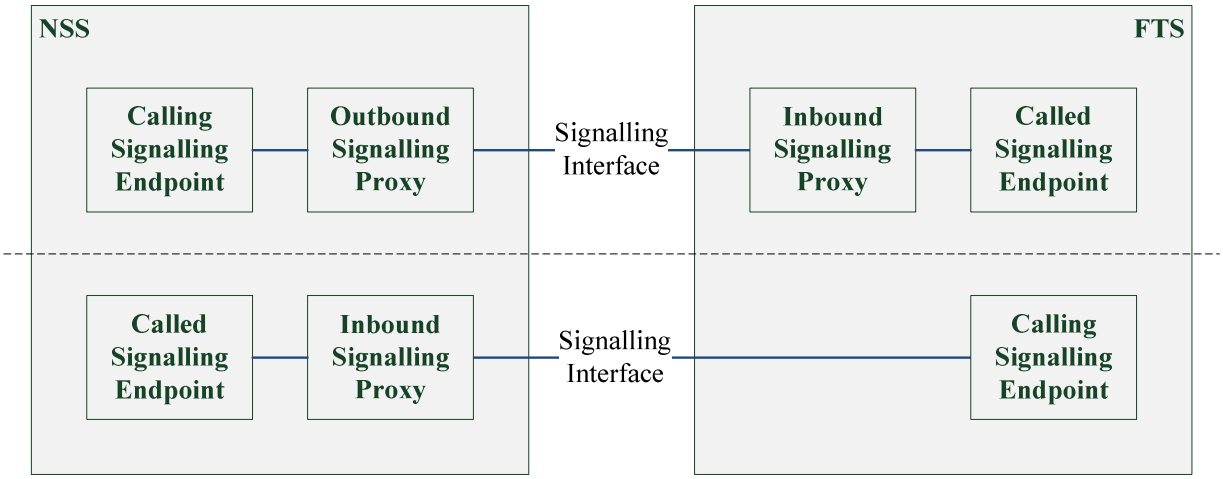
Figure A.1 shows a scenario with no Signalling Proxies deployed. All signalling is directly exchanged between Signalling Endpoints of the FTS and NSS. With respect to this annex and the illustrated deployment scenario the FTS's/NSS's FQDN shall point to some or all of its Signalling Endpoints.



NOTE: Figure A.1 shows the Signalling Interface and the signalling path separately for each call direction. The Signalling Endpoints are qualified with the terms "called" or "calling" to indicate the call direction. This (logical) representation is used to enhance the readability of the diagrams and does not favour any physical implementation.

Figure A.1: Deployment Scenario Endpoints

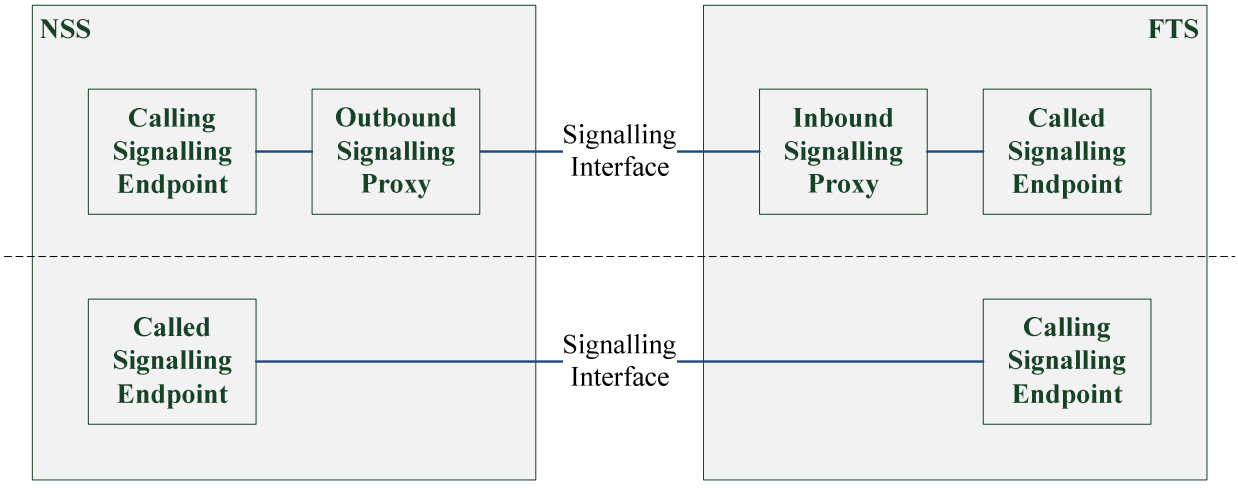
Figure A.2 shows a deployment scenario where both NSS and FTS feature Signalling Proxies in their respective subsystem architecture. The NSS uses its Signalling Proxies for both outgoing and incoming traffic as Outbound and Inbound Signalling Proxies respectively. The FTS uses its Signalling Proxies for incoming traffic only. With respect to this annex and the illustrated deployment scenario the FTS's/NSS's FQDN shall point to its respective Inbound Signalling Proxies and shall not point to any Signalling Endpoint in the subsystem.



NOTE: Figure A.2 shows the Signalling Interface and the signalling path separately for each call direction. The Signalling Endpoints are qualified with the terms "called" or "calling" to indicate the call direction. This (logical) representation is used to enhance the readability of the diagrams and does not favour any physical implementation.

Figure A.2: Deployment Scenario Proxies

Figure A.3 again shows a deployment scenario where both NSS and FTS feature Signalling Proxies in their respective subsystem architecture. In contrast to the example illustrated in figure A.2 the NSS uses its Signalling Proxies for outgoing traffic only whereas the FTS uses its Signalling Proxies for incoming traffic only. With respect to this annex and the scenario in figure A.3 the FTS's FQDN shall point to its respective Inbound Signalling Proxies and the NSS's FQDN shall point to some or all of its Signalling Endpoints.



NOTE: Figure A.3 shows the Signalling Interface and the signalling path separately for each call direction. The Signalling Endpoints are qualified with the terms "called" or "calling" to indicate the call direction. This (logical) representation is used to enhance the readability of the diagrams and does not favour any physical implementation.

Figure A.3: Deployment Scenario Endpoints and Proxies

As the network layer protocol at the present interface is IPv4 (compare clause 6.1) and IP addresses are required to route network traffic, "pointing to all SIP entities" in the previous paragraph means that it is required to resolve a SIP URI hostpart's FQDN to a list of IP addresses, each one representing a possible target for a call.

A specific or homogenous implementation of the name resolution procedure at the SIP entities is not required by the present document. Just to provide a few examples: This may be implemented as proprietary application parameter(s), based on the Domain Name System (DNS) and DNS A resource records (RFC 1035 [i.14] and RFC 2181 [i.15]) or any other concept.

After resolving the Request-URI's hostpart FQDN to a list of IP addresses the source subsystem shall choose one IP address and use it as the target for its call.

How SIP proxies and SIP Endpoints locate each other within the same subsystem is out of scope of the present document and subject to the FTS or NSS design.

Annex B (informative): Quality of Service framework

Depending on the deployment scenario, specifically the type of network connection between FTS and NSS, implementation of Quality of Service mechanisms might become necessary at this interface and the interconnecting network. The Quality of Service framework defined in this annex is the recommended solution to be implemented by the FTS and NSS.

The Quality of Service (QoS) framework at the present interface should be based on the Differentiated Service (DiffServ) Architecture as specified in RFC 2474 [18] and RFC 2475 [19]. DiffServ provides methods of categorizing traffic into classes by marking the type of service (ToS) byte of the IP header with Differentiated Service Code Points (DSCP) as defined in RFC 2474 [18]. This allows the network to handle marked traffic according to an implemented QoS policy. Such a QoS policy is deployment and application specific and thus not the subject of the present document. The present document, in particular this annex, recommends the mechanisms to be used when implementing such a policy at the present interface.

Specific forwarding treatments, formally called Per-Hop Behaviour (PHB), are applied to classified packets by each network element, processing the packet within the appropriate delay-bounds, jitter-bounds etc. and allocating appropriate bandwidth. This combination of packet marking and well-defined PHBs results in a scalable and deterministic QoS solution for any given packet, and any application.

It is the responsibility of the network operator to properly provision transport network equipment and to design the transport network.

At the NSS-FTS interface there are two major types of traffic: signalling and media.

SIP provides application layer retransmission mechanisms, nevertheless it is most important to reduce to a minimum the loss of signalling packets by using a QoS implementation. This results in less signalling errors in case of bandwidth exhaustion and hence in a more deterministic signalling and timing behaviour.

For the media (voice) traffic it is most important to ensure constant and minimal delay and hence minimal jitter. In addition a QoS policy at the present interface should be able to prioritize media traffic according the operational needs and call priority. Call priorities at the present interface are specified in clause 6.4.5.

The NSS and FTS operators can agree on the supported service classes and perform the necessary provisioning tasks to support these service classes at the present interface.

Following the recommendation of RFC 4594 [20] the IP packets, which carry the RTP streams, can be classified with the telephony service class using DSCP value 101110 and Codepoint Expedited Forwarding (EF). In order to allow preferred treatment of media traffic, which belongs to an emergency call, those IP packets should be classified as admitted telephony service class, as defined by RFC 5865 [21]. The media traffic classification can be in line with the network operators call traffic model. The SIP signalling traffic can be marked with DSCP value 100010 and Codepoint Assured Forwarding (AF41).

Table B.1 shows the recommended mapping of the applications to the DSCP values; other mappings are allowed based on bilateral agreement.

Table B.1: DSCP mapping example

Application	DSCP value	Codepoint
Default	000000	CS0
Telephone voice (priority 1 to 4)	101110	EF
Telephone voice (priority 0)	101100	Voice Admit
Signalling	100010	AF41

Annex C (informative): Security Framework

This annex defines the security mechanisms that should be implemented by FTS and NSS with respect to the present interface.

The NSS, FTS and the interconnecting network can implement sufficient security principles and mechanisms in order to build a valid, overall security concept together with the minimum security mechanisms for the present interface.

System security principles, requirements and mechanisms for the FTS and the NSS itself are out of scope of the present document, as are transport network security principles, requirements and mechanisms.

At the time of the creation of the present document, real world deployment scenarios allow for the following assumptions to be made:

- Unauthorized physical access protection for the NSS, FTS and transport network equipment is covered by the execution of very rigid operational and facility security policies. Thus neither unauthorized and unapproved access to existing equipment nor the connection of unauthorized and unapproved equipment to the existing systems and networks is possible.
- NSS and FTS are using the same (transport) network infrastructure for internal and external communication. The network infrastructure completely isolates this communication from any other network application than GSM-R from the network layer upwards.
- The (transport) network equipment is being protected by strong and state of the art security mechanisms. Thus any access from out of domain systems and networks is impossible.
- NSS and FTS implement strong and state of the art system security mechanisms protecting the system as well as any interconnected equipment from unauthorized access.

This means all networking equipment, its purpose and configuration, connected to the operating environment for the interface subject to the present document is known, validated and approved by the network operator. Such an operating environment is referred to in the present document as a trusted environment.

This annex focuses on the security requirements in a trusted environment. Security requirements, design and implementation guidelines for an environment other than a trusted environment may be addressed by a future release of the present document.

Information security has various dimensions and aspects. Due to the nature of the trusted environment at the present interface a single security issue will be addressed at the present interface: Authorization.

Authorization of Signalling Entities at the present interface can be based on IP address verification. Both the FTS and NSS Signalling Endpoints can hold a statically configured access control list, containing the IP addresses of all approved signalling partners at the other side of the interface. These are SIP endpoints and SIP proxies. All Signalling Entities can verify all incoming signalling message against this access control list. Any unauthorized signalling message can be rejected or ignored. Signalling Entities can verify the previous hop's IP address at the IP protocol (Internet layer) level. Signalling Entities may additionally verify IP addresses at the SIP protocol level.

Authorization of Media Endpoints is out of scope of the present document, as they are under full control of the Signalling Endpoints with respect to the present interface.

Annex D (informative): Mapping of EIRENE to Interface Features

Tables D.1, D.2 and D.3 list the services as required by EIRENE [1] and indicate whether these services are supported (M) on the SIP based interface between NSS and FTS or not (-).

Bearer Services are not supported at the present interface.

Table D.1: Teleservices

Category		Teleservice	Support	Note
Group Number	**Service Name**			
1	Speech Transmission	11 - Telephony	M	
		12 - Emergency calls	M	
2	Short Message Service	21 - Short message MT/PP	-	Out of scope of the present interface
		22 - Short message MO/PP	-	Out of scope of the present interface
		23 - Short message cell broadcast	-	Out of scope of the present interface
6	Facsimile Transmission	61 - Alternate speech and fax group 3	-	Currently out of scope, to be considered in future
		62 - Automatic fax group 3	-	Currently out of scope, to be considered in future
9	Voice Group service	91 - Voice Group Call Service (VGCS)	M	Is treated as point to point session at the present interface
		92 - Voice Broadcast Service (VBS)	M	Is treated as point to point session at the present interface
NOTE: Group Numbers and numbers of Teleservices are shown in this table as listed in EIRENE [1].				

Table D.2: Supplementary Services

Supplementary Service	Support	Note
Calling Line Identification Presentation (CLIP)	M	
Calling Line Identification Restriction (CLIR)	-	Currently out of scope, to be considered in future
Connected Line Identification Presentation (CoLP)	M	
Connected Line Identification Restriction (CoLR)	-	Currently out of scope, to be considered in future
Call Forwarding Unconditional (CFU)	-	Only number update supported, but not the forwarding as such
Call Forwarding on Mobile Subscriber Busy (CFB)	-	Only number update supported, but not the forwarding as such
Call Forwarding on No Reply (CFNRy)	-	Only number update supported, but not the forwarding as such
Call forwarding on Mobile Subscriber Not Reachable (CFNRc)	-	Only number update supported, but not the forwarding as such
Call waiting (CW)	Implicit	
Call hold (HOLD)	M	
Multi Party Service (MPTY)/Conference	-	Out of scope, pure NSS/FTS feature
Closed User Group (CUG)	-	Out of scope of the present interface
Advice of Charge (Information) (AoCI)	-	Out of scope of the present interface
Advice of Charge (Charging) (AoCC)	-	Out of scope of the present interface
Barring of All Outgoing Calls (BAOC)	-	Out of scope of the present interface
Barring of Outgoing International Calls (BOIC)	-	Out of scope of the present interface
BOIC except those to Home PLMN Country (BOIC-exHC)	-	Out of scope of the present interface
Barring of All Incoming Calls (BAIC)	-	Out of scope of the present interface
Barring of Incoming Calls when Roaming Outside the Home PLMN Country (BIC-Roam)	-	Out of scope of the present interface
Unstructured Supplementary Service Data (USSD)	-	Not applicable at the present interface
Sub-addressing	-	Out of scope of the present interface
Enhanced Multi-Level Precedence and Pre-emption (eMLPP)	M	
Explicit Call Transfer (ECT)	-	Only number update supported, but not the forwarding as such
Completion of Calls to Busy Subscribers (CCBS)	-	Currently out of scope, may be considered in future
User-to-User Signalling 1 (UUS1)	M	

Table D.3: Railway Services

Railway Service	Support	Note
Functional addressing	M	
Location dependent addressing	-	Out of scope of the present interface
Shunting mode	-	Out of scope of the present interface
Multiple driver communications	-	Out of scope of the present interface
Emergency calls	M	Means "Railway Emergency Calls"

Annex E (informative): Group Call Control Scenarios

As described in clause 5.5 of the present document VGCS/VBS are provided by the NSS. The present interface provides mechanisms for the FTS to control VGCS/VBS calls from the perspective of fixed terminal users, such as termination of VGCS/VBS and requests for mute/unmute of the mobile terminal downlink of VGCS.

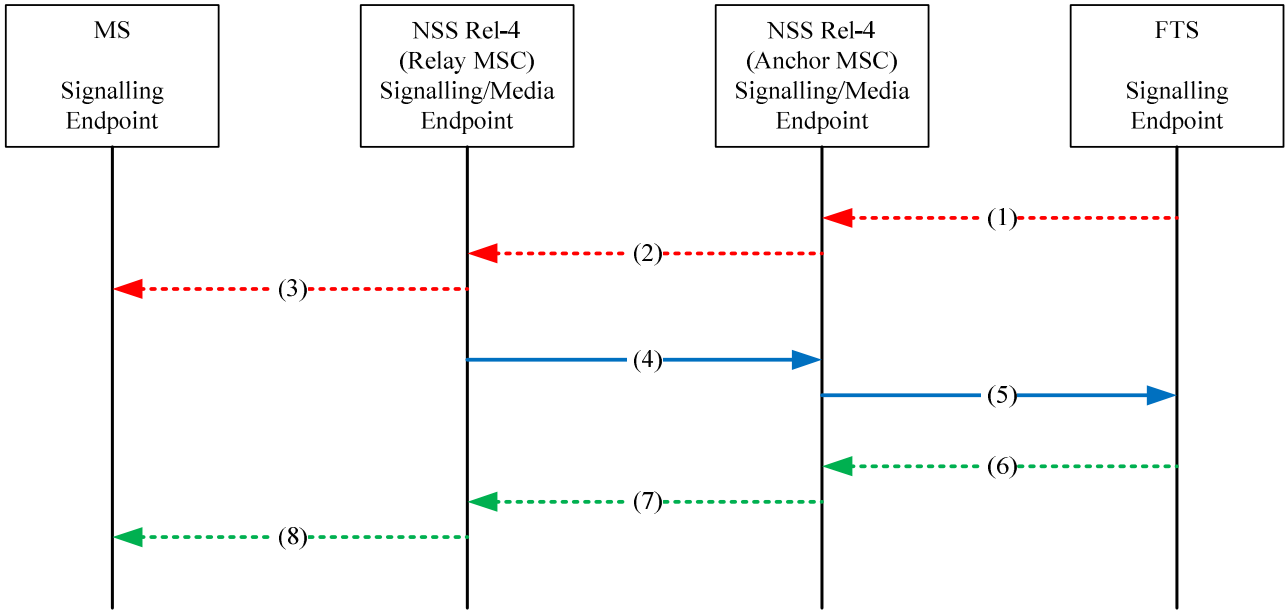
On the interface between or within core networks, the engaged MSCs may use message based DTMF signalling (out-band signalling) or DTMF tones (in-band signalling):

- In core networks based on Rel-4 architecture, message based DTMF signalling is used.
- In core networks based on Rel-99 architecture, DTMF tones are used.
- In a mixed core network architecture (Rel-4 and Rel-99) DTMF tones are used.

Therefore the present interface supports message based explicit signalling as well as DTMF tones:

- For implementations including only core networks based on Rel-4 architecture, message based explicit signalling is recommended to be used (see clause 6.4.11).
- For mixed implementations or for implementations including only core networks based on Rel-99 architecture, DTMF tones are recommended to be used (see clause 7.4.1).

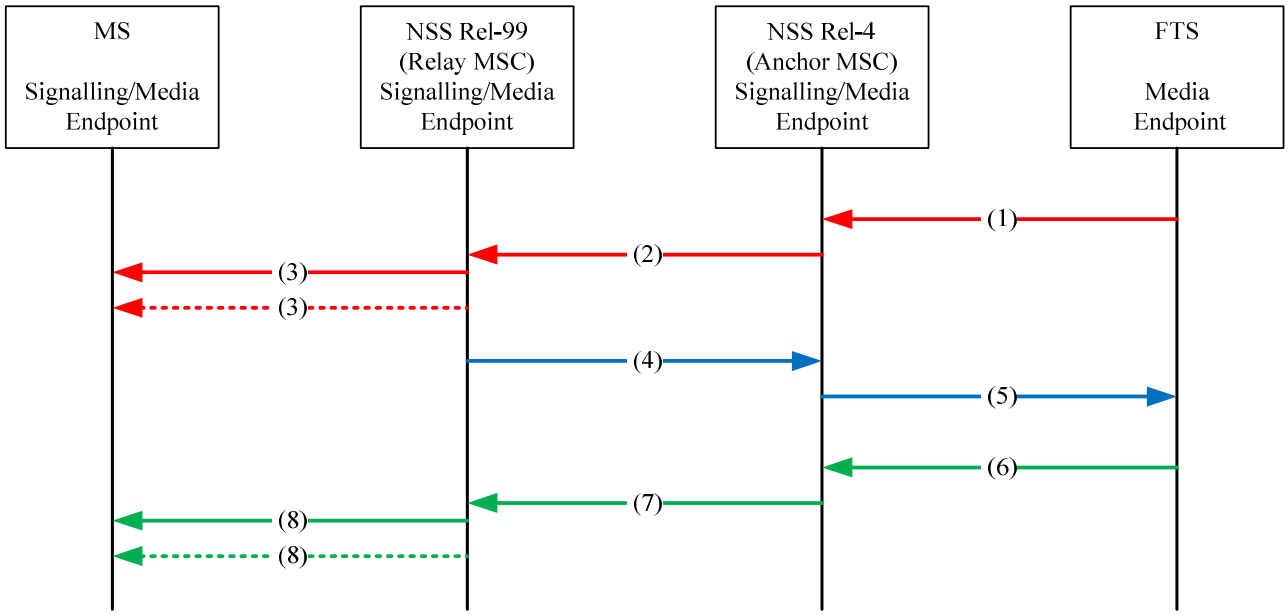
Figure E.1 shows the usage of explicit signalling for VGCS/VBS control for an implementation including only core networks based on Rel-4 architecture:



NOTE:
(1) Muting Control: SIP based explicit signalling (out-band)
(2) Muting Control: message based DTMF signalling (out-band)
(3) Muting Control: set parameter message (out-band)
(4) Grant: tones via RTP stream (in-band)
(5) Grant: tones via RTP stream (in-band)
(6) Termination: SIP based explicit signalling (out-band)
(7) Termination: message based DTMF signalling (out-band)
(8) Termination: termination message (out-band)

Figure E.1: Group Call Indication via message based explicit signalling for CN Rel-4

Figure E.2 shows the usage of DTMF tones for VGCS/VBS control for an implementation including core networks based on Rel-99 and Rel-4 architecture:



NOTE:
(1) Muting Control: DTMF tones via RTP stream (in-band)
(2) Muting Control: DTMF tones via in-band signalling
(3) Muting Control: DTMF tones (in-band) followed by set parameter message (out-band)
→ Tones hearable by all VGCS subscribers, except talker in case no DL is used
(4) Grant: tones via in-band signalling (in-band)
(5) Grant: tones via RTP stream (in-band)
(6) Termination: DTMF tones via RTP stream (in-band)
(7) Termination: DTMF tones via in-band signalling
(8) Termination: DTMF tones (in-band) followed by termination message (out-band)
→ Tones hearable by all VGCS subscribers, except talker in case no DL is used

Figure E.2: Group Call Indication via DTMF tones for mixed CN Rel-99 and Rel-4

The issue and possible solutions for the VGCS related DTMF problem "DTMF tones hearable by listeners" is out of scope of the present document.

Annex F (informative): Bibliography

IETF RFC 2597 (1999): "Assured Forwarding PHB Group".

IETF draft RFC draft-jones-sip-options-ping-02: "Using OPTIONS to Query for Operational Status in the Session Initiation Protocol (SIP)".

History

Document history		
V1.1.1	September 2011	Publication
V1.2.1	September 2013	Publication
V2.0.0	August 2014	Publication