Technical Technical Specification of the SIP (Gm) interface between the User Equipment (UE) and the IMS platform of Deutsche Telekom

1 TR 114

Version V4.3.0

7. March 2024

Publisher

Deutsche Telekom Technik GmbH

Responsible

Deutsche Telekom Technik GmbH

Services and Platforms

One VM Design

64307 Darmstadt

Order Information

Title: 1 TR 114

Version: 4.3.0. (March 2024)

Replacement for 1 TR 114, Version 4.2.0

Order Address

Deutsche Telekom Technik GmbH

Services and Platforms

One VM Design

64307 Darmstadt

Contents

Foreword

This Technical Specification (Technische Richtlinie, TR) has been produced by the department One VM Design of Deutsche Telekom Technik GmbH, Services & Platforms (in the following named as Deutsche Telekom) and contains the description of the SIP (Gm) interface between a User Equipment (UE) and the IMS platform of Deutsche Telekom.

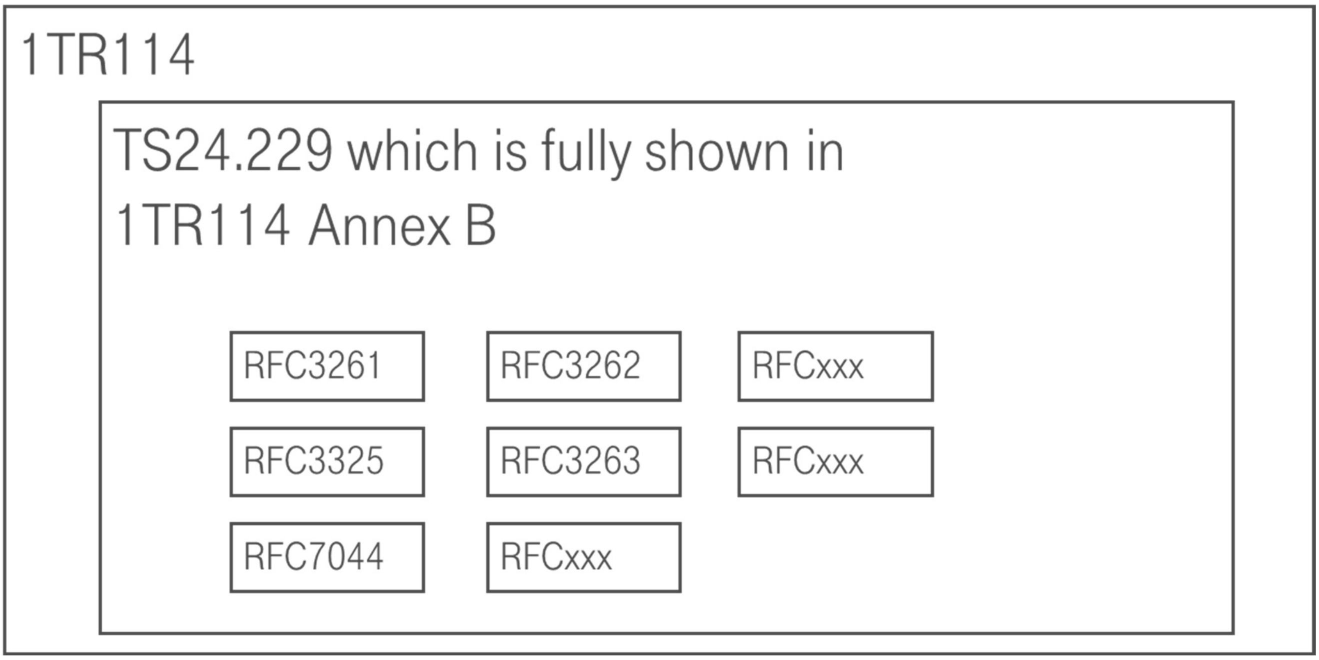
The Gm reference point supports the communication between UE and NGN platform of Deutsche Telekom, e.g. related to registration and session control.

The protocol used for the Gm reference point is SIP (as defined by RFC 3261 [71], other relevant RFCs, and additional enhancements introduced to support 3GPPs needs).

Annex A of the present document is no longer valid.

Annex B of the present document is an endorsement specification based on the 3GPP Technical Specification TS 24.229 Release 11 [21] (endorsement).

The figure below shows the principle of endorsement used within this document.



1 Scope

The present Technical Specification (TR) is applicable to the SIP (Gm) interface between a User Equipment (UE) and the Next Generation Network (IMS) of Deutsche Telekom according to the AGB [1] of Deutsche Telekom.

The present document does not describe the physical characteristics and transmission requirements via the subscriber line.

A possible physical access is e.g. an xDSL interface provided by Deutsche Telekom which is described in the technical specification 1TR112.

Reference points of 1TR114 Figure 1-1 shows the scope of the relevant technical specifications.

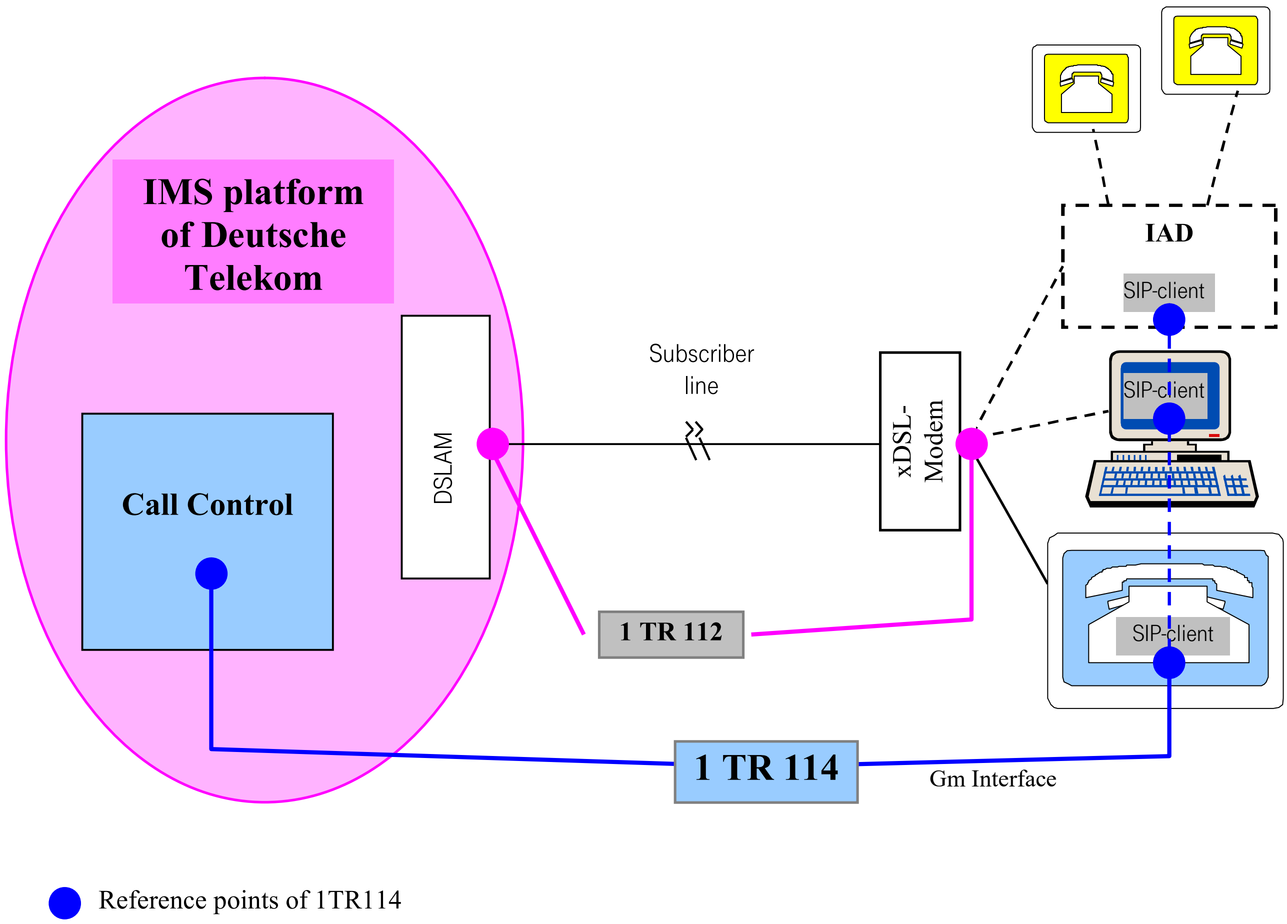


Figure 1-1: Scope of the relevant technical specifications

2 References

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

References are either specific (identified by date of publication and/or edition number or version number) or non specific.

- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version including amendments, errata and corrigenda applies.

Date of publication in square brackets [ ] refer just to the last known version while this document was in revision.

[1] AGB: Allgemeine Geschäftsbedingungen der Deutschen Telekom
(see: www.telekom.de/agb)

[2] DT 1TR112: Technical Specification of the Broadband-Access-Interfaces in the network of Deutsche Telekom

[3] DT 1TR126: Technical Specification for SIP User Equipments (UE) providing IMS simulation services via analogue (POTS) interfaces (POTS/SIP interworking) using the IMS platform of Deutsche Telekom

[4] DT 1TR127: Technical Specification for SIP User Equipments (UE) providing IMS simulation services via ISDN (DSS1) interfaces (ISDN/SIP interworking) using the IMS platform of Deutsche Telekom

[5] ETSI TS 102 144 V1.1.1 (2003-05): Services and Protocols for Advanced Networks (SPAN);
MTP/SCCP/SSCOP and SIGTRAN (Transport of SS7 over IP);
Stream Control Transmission Protocol (SCTP)
[Endorsement of RFC 2960 and RFC 3309, modified]

[6] 3GPP TS 24.606: "Message Waiting Indication (MWI) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification"(Release 11).

[7] 3GPP TS 24.607: "Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification"(Release 11).

[8] 3GPP TS 24.608: "Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification"(Release 11).

[9] 3GPP TS 24.611: "Anonymous Communication Rejection (ACR) and Communication Barring (CB) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification"(Release 11).

[10] 3GPP TS 24.647: "Messaging using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3"(Release 11).

[11] Void

[12] 3GPP TS 24.604: "Communication Diversion (CDIV); Protocol specification using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification "(Release 11).

[13] 3GPP TS 24.608: "Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification"(Release 11).

[14] 3GPP TS 24.616 V11.1.0 (2012-12): 3rd Generation Partnership Project;Technical Specification Group Core Network and Terminals;Malicious Communication Identification (MCID) using IP Multimedia (IM) Core Network (CN) subsystem;Protocol specification (Release 11)

[15] 3GPP TS 24.629: "Explicit Communication Transfer (ECT) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification"(Release 11).

[16] 3GPP TS 24.605: "Conference (CONF) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification"(Release 11).

[17] 3GPP TS 24. 628 V11.2.0 (2012-12): Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Common Basic Communication procedures using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (Release 11)

[18] 3GPP TS 23.060 V11.5.0 (2013-03): Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2 (Release 11)

[19] 3GPP TS 23.228: Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 11)

[20] 3GPP TS 23.401 V11.5.0 (2013-03): Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (Release 11)

[21] 3GPP TS 24.229 V11.6.0 (2012-12): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 11)

[22] 3GPP TS 24.615: 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Communication Waiting (CW) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification; (Release 11)

[23] 3GPP TS 24.642 : 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Completion of Communications to Busy Subscriber (CCBS) Completion of Communications by No Reply (CCNR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification; (Release 11)

[24] 3GPP TS 29.163 v11.5.0 (2012-12): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Interworking between the IP Multimedia (IM) Core Network (CN) subsystem and Circuit Switched (CS) networks (Release 11)

[25] ITU-T E.164 (02/2005): OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS; International operation – Numbering plan of the international telephone service; The international public telecommunication numbering plan

[26] ITU-T G.711 (11/1988): GENERAL ASPECTS OF DIGITAL TRANSMISSION SYSTEMS, TERMINAL EQUIPMENT, Pulse code modulation (PCM) of voice frequencies

[27] ITU-T G.722 (1993): GENERAL ASPECTS OF DIGITAL TRANSMISSION SYSTEMS, TERMINAL EQUIPMENT, 7 kHz AUDIO – CODING WITHIN 64 KBIT/S

[28] ITU-T H.261 (03/93): LINE TRANSMISSION OF NON-TELEPHONE SIGNALS; VIDEO CODEC FOR AUDIOVISUAL SERVICES AT p x 64 kbits

[29] ITU-T H.263 (01/2005): AUDIOVISUAL AND MULTIMEDIA SYSTEMS; Infrastructure of audiovisual services – Coding of moving video ; Video coding for low bit rate communication

[30] ITU-T H.264 (11/2007): AUDIOVISUAL AND MULTIMEDIA SYSTEMS; Infrastructure of audiovisual services – Coding of moving video; Advanced video coding for generic audiovisual services

[31] ITU-T T.30 (09/2005): TERMINALS FOR TELEMATIC SERVICES; Procedures for document facsimile transmission in the general switched telephone network

[32] ITU-T T.38 (04/2007): TERMINALS FOR TELEMATIC SERVICES; Facsimile – Group 3 protocols; Procedures for real-time Group 3 facsimile communication over IP networks

[33] ITU-T V.152 (01/2005): DATA COMMUNICATION OVER THE TELEPHONE NETWORK; Interworking with other networks; Procedures for supporting voice-band data over IP networks

[34] IETF RFC 0768: User Datagram Protocol; 28 August 1980

[35] IETF RFC 0791: INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION; September 1981

[36] IETF RFC 0792: INTERNET CONTROL MESSAGE PROTOCOL; September 1981

[37] IETF RFC 0793: TRANSMISSION CONTROL PROTOCOL; DARPA INTERNET PROGRAM; PROTOCOL SPECIFICATION; September 1981

[38] IETF RFC 1035: DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION; November 1987

[39] IETF RFC 2032: RTP Payload Format for H.261 Video Streams; October 1996

[40] IETF RFC 2046: Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types; November 1996

[41] IETF RFC 2190: RTP Payload Format for H.263 Video Streams; September 1997

[42] IETF RFC 5246: The Transport Layer Security (TLS) Protocol; Version 1.2; January 2008

[43] IETF RFC 2327: SDP: Session Description Protocol; April 1998

[44] IETF RFC 2411: IP Security Document Roadmap; November 1998

[45] IETF RFC 2429: RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video (H.263+); October 1998

[46] IETF RFC 2460: Internet Protocol, Version 6 (IPv6) Specification; December 1998

[47] IETF RFC 2782: A DNS RR for specifying the location of services (DNS SRV); February 2000

[48] IETF RFC 2915: The Naming Authority Pointer (NAPTR) DNS Resource Record; September 2000

[49] IETF RFC 3041: Privacy Extensions for Stateless Address Autoconfiguration in IPv6; January 2001

[50] IETF RFC 3263: Session Initiation Protocol (SIP): Locating SIP Servers; June 2002

[51] IETF RFC 3316: Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts; April 2003

[52] IETF RFC 3362: Real-time Facsimile (T.38) - image/t38; MIME Sub-type Registration; August 2002

[53] IETF RFC 3550: RTP: A Transport Protocol for Real-Time Applications; July 2003

[54] IETF RFC 3596: DNS Extensions to Support IP Version 6; October 2003

[55] IETF RFC 3842: A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP); August 2004

[56] IETF RFC 3858: An Extensible Markup Language (XML) Based Format for Watcher Information; August 2004

[57] IETF RFC 3863: Presence Information Data Format (PIDF); August 2004

[58] IETF RFC 3890: A Transport Independent Bandwidth Modifier for the Session Description Protocol (SDP); September 2004

[59] IETF RFC 3966: The tel URI for Telephone Numbers; December 2004

[60] IETF RFC 3984: RTP Payload Format for H.264 Video; February 2005

[61] IETF RFC 4028: Session Timers in the Session Initiation Protocol (SIP); April 2005

[62] IETF RFC 4040: RTP Payload Format for a 64 kbit/s Transparent Call; April 2005

[63] IETF RFC 4122: A Universally Unique IDentifier (UUID) URN Namespace; July 2005

[64] IETF RFC 4443: Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification; March 2006

[65] IETF RFC 4733: RTP Payload for DTMF Digits, Telephony Tones, and Telephony Signals; December 2006

[66] IETF RFC 4734: Definition of Events for Modem, Fax, and Text Telephony Signals; December 2006

[67] IETF RFC 5244: Definition of Events for Channel-Oriented Telephony Signalling; June 2008

[68] IETF RFC 5626: Managing Client-Initiated Connections in the Session Initiation Protocol (SIP); October 2009

[69] IETF RFC 5627: Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP); October 2009

[70] IETF RFC 4884: Extended ICMP to Support Multi-Part Messages, April 2007

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

[72] Broadband Forum TR-069 "CPE WAN Management Protocol"

[73] Broadband Forum TR-104 "DSLHome Provisioning Parameters for VoIP CPE"

[74] Broadband Forum TR-181 "Device Data model for TR-069",

[75] 3GPP TS 23.003: "Numbering, addressing and identification".

[76] RFC 3711: The Secure Real-time Transport Protocol (SRTP), March 2004

[77] RFC 4568 (July 2006): "Session Description Protocol (SDP) Security Descriptions for Media Streams".

[78] RFC 4347 (April 2006) "Datagram Transport Layer Security"

[79] IETF draft-dawes-dispatch-mediasec-parameter-07.txt "Security Mechanism Names for Media"

[80] BSI Technische Richtlinie TR-02102-2 "Kryptographische Verfahren: Empfehlungen und Schlüssellängen; Teil 2 – Verwendung von Transport Layer Security (TLS)" Version 2014-01(12.02.2014)

[81] RFC 3713 – A Description of the Camellia Encryption Algorithm

[82] RFC 3657 – Use of the Camellia Encryption Algorithm in Cryptographic Message Syntax (CMS)

[83] RFC 5639 - Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation

[84] RFC 7027 (October 2013) - Elliptic Curve Cryptography (ECC) Brainpool Curves for Transport Layer Security (TLS)

[85] RFC 6066 (Januar 2011) - Transport Layer Security (TLS) Extensions: Extension Definitions

[86] RFC 5746 (February 2010) - Transport Layer Security (TLS) Renegotiation Indication Extension

[87] RFC 5289 (August 2008) - TLS Elliptic Curve Cipher Suites with SHA-256/384 and AES Galois Counter Mode (GCM)

[88] RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2

[89] RFC 5288 (August 2008) AES Galois Counter Mode (GCM) Cipher Suites for TLS

[90] RFC 5923 (June 2010) Connection Reuse in the Session Initiation Protocol (SIP)

[91] DT 1TR118 Technical Specification of the SIP-Trunking Interface between a SIP-PBX with DDI and the NGN Platform of Telekom Deutschland

[92] DT 1TR119 Technical Specification of the SIP-Trunking Interface for CompanyFlex

[93] 3GPP TS 23.002: "Network architecture".

[94] RFC 4961 (Juli 2007) Symmetric RTP / RTP Control Protocol (RTCP)

[95] RFC 5280 (May 2008) Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

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

[142] RFC 6228 (May 2011): "Response Code for Indication of Terminated Dialog".

[200] TR-02102-1 BSI: Technische Richtlinie TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, 2021

[201] RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3, August 2018

3 Definitions and Symbols Definitions

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

Term	Definition / Remark
Call Control	In telephony, call control refers to the software within a telephone switch that supplies its central function. Call control decodes addressing information and routes telephone calls from one end point to another. It also creates the features that can be used to adapt standard switch operation to the needs of users. Call control software, because of its central place in the operation of the telephone network, is marked by both complexity and reliability.
End Device	An End Device seen from IAD perspective could be: 1. A POTS phone, i.e. each analogue end device connected has its port number. 2. ISDN phone or terminal adapter. Depending on the implementation each ISDN Phone may have a port number or equivalent. The ISDN Adapter may have two virtual port number per S0 channel supported which may be dynamically provided. This is implementation depended. 3. DECT phone. For each DECT phone a Port Number. 4. Or any other device used for telephony which interacts with an IAD SIP UA or is acting as IAD SIP UA or UA.
Gm	Referenc point of SIP Interface between User Equipment and Deutsche Telekom IMS. 1TR114 is describing this reference point.
GRUU	Global Routable URI. Within the scope of this document a GRUU shall be generated for each IAD SIP UA i.e the combination of contacted end device/ Port Number. For this document a self made GRUU as defined in RFC 5627 [53] shall apply.
IAD SIP UA	A IAD SIP UA is a naming within this document to reflect the combination of IMPU and Port number. This IAD SIP UA may register at the SIP UA “virtually” or “real”. How this procedure is done is due to the implementation. Dependent on implementation the IAD SIP UA may be the same function as the SIP UA.
NGN platform (of Deutsche Telekom)	The IP Multimedia System (IMS) is an architectural framework for delivering IP multimedia services. IMS uses IETF protocols wherever possible, e.g., the Session Initiation Protocol (SIP). According to the 3GPP, IMS is intended to access multimedia and voice applications from wireless and wireline terminals. Within the scope of this document with IMS the Platform of Deutsche Telekom providing the multimedia and telephony services for fixed line access is meant.
IP	Considering the expected parallel availability of IPv4 and IPv6 the term “IP” in this document is related to both internet protocol versions.

Term	Definition / Remark
Media Authorization	Media Authorization is related to the use of P-Early-Media Header as defined in RFC5009 [109] Early media is authorized by the network, if and only if there is at least one early dialog for which • SDP (answer) has been received from network and • the last (backward) P-EARLY-MEDIA header provided a value from set {sendonly, sendrecv, recvonly}. Backward early media is authorized by the network, if and only if there is at least one early dialog for which • SDP (answer) has been received from network and • the last (backward) P-EARLY-MEDIA header provided a value from set {sendonly, sendrecv}. Forward early media is authorized by the network, if and only if there is at least one early dialog for which • SDP (answer) has been received from network and • the last (backward) P-EARLY-MEDIA header provided a value from set {sendrecv, recvonly}. In case of SDP (answer) has been received, but no P-EARLY-MEDIA header has been received for the given dialog with any message an implicit P-EARLY-MEDIA=sendonly shall be assumed. P-EARLY-MEDIA header shall be considered independent whether the P-EARLY-MEDIA header has been received by means of a reliable or unreliable response. The term of local ringtone used within this documentation is the same as a locally generated ringback tone (RBT). More information how to generate a local ringtone is given in ANNEX E of 1TR114
Port Number	Port number defined for this Amendment document is a unique identifier which is used for a physical or virtual interface to connect a SIP UA with an End Device.
SIP UA	This is the SIP UA acting as contact point towards the IMS Gm. The SIP UA is responsible for registering the IMPU’s at the IMS (i.e. Registrar). Depended on implementation within the IAD the SIP UA may act as internal SIP registrar and forking Proxy against the port number/IMPU combination as defined below.
Shall	As usual within standards and documents of Deutsche Telekom, 3GPP, ETSI and ITU-T the word shall is used to indicate a procedure or requirement as mandatory. A definition is also given in RFC2119.
Should	As usual within standards and documents of Deutsche Telekom, 3GPP, ETSI and ITU-T the word should is used to indicate a procedure or requirement as optional. A definition is also given in RFC2119.

Term	Definition / Remark
User Agent (UA)	Definition is given in RFC3261. A client application used with a particular network protocol, such as Session Initiation Protocol (SIP); it refers to both end points of a phone call, server and client. Within the scope of this document the SIP User Agent (UA) is acting as contact point towards the IMS Gm reference point as defined in TS 23.002 [93]. The SIP UA is responsible for registering the IMPU's at the IMS (i.e. Registrar). Depended on implementation within the IAD the SIP UA may act as internal SIP registrar and forking Proxy against the port number/IMPU combination as defined below.
User Equipment (UE)	Any SIP device (terminal) at the subscriber premises used by an end user to communicate. It can be e.g. an IAD or telephone set, or any other telecommunication device.
VoIP line	A VoIP line is equivalent to a MSN in ISDN; Multiple VoIP lines can be assigned to a VoIP account of the NGN platform of Deutsche Telekom.

3.1 Symbols

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

Symbol	Definition
*	Star sign
#	Hash sign
	Pick-up the receiver (Off-hook)
	Hang-up the receiver (On-hook)
	Hook Flash (flash hook function) (procedure to invoke "register recall"); In case of a SIP UE it shall invoke an equivalent SIP procedure according to the service specifications as described in Annex C.
< >	Information in pointed brackets is an obliged variable input (signs or figures)

4 General Description

4.1 Introduction

The Deutsche Telekom voice platform is a IP Multimedia Subsystem (IMS) using the SIP protocol as defined by 3GPP.

The subscriber needs a suitable terminal (User Equipment) to be able to use the SIP-based telephony services via the NGN platform of Deutsche Telekom. These terminals can be either hard phones, adaptors or soft phones.

- A hard phone is a conventional telephone but with an interface for connecting to an IP network.
- In addition, routers (with an integrated DSL modem) and adaptors are commercially available which allow conventional telephones to be used for Internet telephony by means of a special interface (IAD). The IMS platform of Deutsche Telekom also supports these integrated adapters. Legacy TDM and ISDN-terminals can still be operated in the customer-area via such adapters.
- A soft phone is the name given to application software which allows a PC to perform SIP-based telephony over the Internet.

This document describes the baseline for SIP UEs connected via a PBX either directly connected via the Deutsche Telekom Gm reference point/interface as described within this document as well as connected via the Deutsche Telekom SIP Trunk product described within 1TR118 [91] and 1TR119 [92]. Deviations and the architectural aspects for Deutsche Telekom SIP Trunk products from this document will be described within 1TR118 [91] and 1TR 119 [82].

4.2 Capabilities

4.2.1 General Requirements and SIP capabilities

The Re-Ringing procedure for the SIP UE shall apply according to 1TR126 [3]. (This feature may not apply in combination with 1TR118 [91])

The Protocol stacks shall work with IPv4 and IPv6.

Neither UICC nor ISIM is applicable for this document.

ICSI and IARI shall be passed on in compliance with the current specification.

Support of session timers regarding RFC 4028 [61] is mandatory.

For tones and announcements, the procedures described in 3GPP TS 24.628, Annex D [17] shall apply. The bidirectional early media shall be used.

Sending of INVITE without SDP for call setup procedures are not supported by the IMS core of Deutsche Telekom.

The restoration procedures as described within ANNEX B shall be supported.

Authentication shall be possible via HTTP Digest and without HTTP Digest (NASS bundled) based on the line/IP-Address.

NOTE: For SIP trunk according to 1TR118 [91]/1TR119 [92] the service implementation may differentiate. More information is given in 1TR118 [91] /1TR119 [92]

For SIP UE supporting SIP-Analogue and SIP-ISDN interworking (e.g. IAD) the subscription of the "ua-profile" is **implicit.** This overrules the procedures stated within 1TR126 ANNEX A Section "A 5.3.1.2 Subscription for profile delivery" and 1TR127 ANNEX B Section "A 5.3.1.2 Subscription for profile delivery"

The sending of the SUBSCRIBE Method for the "ua-profile" and "MWI package" shall not apply.

The Call-Id presented by the terminating UE shall not include the own IP-address of the UA.

Format of User-Agent-Header The following format for the User Agent Header is strongly Recommended

1. Contains name of Entity
2. Contains Firmware Version of the Entity

4.2.2 URI Formats

Request URI = SIP URI with user=phone shall be used. Tel URI are allowed.

SIP URIs shall be supported in SIP header fields.

Request URI = SIP URI with user=phone is used for SCC like *21%23@hostportion. (This feature may not apply in combination with 1TR118 [91])

HEX digits as defined within RFC 3966 [58] to be sent or received on the Gm interface in SIP URI user=phone are not allowed.

Header fields received may contain tel URI or alias URI as defined in 3GPP TS 23.003 [75]

All URI (Request, From etc.) should be presented within global number format.

(hash) in URIs must be escaped. (This feature may not apply in combination with 1TR118 [91])

For future network improvements the capabilities of registering and sending SIP URI as defined for Public User Identities in 3GPP TS 23.003 [75] SHOULD exist. Currently the only SIP URI's representing a E.164 Number in the host portion. Default is SIP URI with user=phone, are used

Visual separators within URIs shall not be used.

Numbers received in From header shall be displayed. In cases where From header is not usable for rendering the P-Asserted-Identity shall be used instead.

4.2.2.1 Special Service Numbers

Harmonized Services of Social Value Numbers ("Harmonisierte Dienste von Sozialem Wert") are of the form 116xyz (e.g. 116117). These numbers shall be routed with a dedicated routing prefix ("Verkehrslenkungsnummer") (0)1987 followed by the xyz part of the phone number, e.g. +491987117.

To allow international reachability and to offer a displayable dial back option for these numbers, it shall also be possible to dial these numbers with a leading country code and without routing prefix, e.g. +49116117.

The following format shows an example:

sip: +49116xxx@tel.t-online.de

Currently the following numbers are in use or allocated:

- 116000 (Notruf für vermisste Kinder),
- 116111 (Hotlines für Hilfe suchende Kinder),
- 116117 (Bereitschaftsdienst für ärztliche Hilfe in nicht lebensbedrohlichen Situationen),
- 116123 (Hotlines zur Lebenshilfe) sowie
- 116006 (Beratungsdienst für Opfer von Verbrechen)
- 116116 (Sperrung von elektronischen Berechtigungen)

NOTE: Further numbers may be available in future.

P-Asserted-URI and From Header received with such number must be accepted and usable for redialling. From header with such number should be displayed at the UA/IAD.

4.2.3 Invocation of Services

A SIP UE supporting the services provided by the IMS platform of Deutsche Telekom Deutsche Telekom shall use the procedures with the relevant Service Command Codes (SCC) (e.g. *21#). These service procedures (incl. SCC) are described in Annex D of this document. Either the SCC can be directly dialled via the key pad on the SIP Phone or via specific service menu buttons (e.g.: Press button "xyz" for invoking CCBS) which initiates the regarding SCC. The SCC shall be sent in the format of a SIP URI: SCC@hostportion within an initial INVITE. If SIP equivalent procedures are available and supported by the network these shall be preferred. (This feature may not apply in combination with 1TR118 [91] and 1TR119 [92])

Particular services provided by the IMS platform of Deutsche Telekom require specific procedures using Switching Order Commands (SOC). A SIP UE supporting these services shall use the procedures (incl. SOC) which are described in Annex D of this document and 1TR126 [3]. (This feature may not apply in combination with 1TR118 [91] and 1TR119 [92])

The Hook-Flash handling and the invocation of services are described in 1TR126 [3]. The implementation of the procedures for the Hook-Flash handling, if it is a real Hook-Flash or only a menu button to invoke the service; is a matter of the vendor and out of the scope of this document. (This feature may not apply in combination with 1TR118 [91] and 1TR119 [92])

4.2.4 Multimedia Telephony

4.2.4.1 Voice Telephony

Voice over IP (VoIP) is performed in accordance with the SIP-Protocol. The specifications to be fulfilled for control of a communication are presented in section 7.

For the Media-Stream the Codecs G.711a (A-Law) and G.722 shall be used. For VGW (IAD) supporting ISDN accesses RFC 4040 [62] (Clearmode) shall be supported.

To avoid transcoding towards mobile users to AMR-WB Codec as described within 3GPP TS 26.090 [78] and TS 26.190 [80], EVS shall be handled transparently within devices when forwarding the call.

NOTE: An implementation of AMR or EVS is not needed.

A SDP offer shall contain as minimum G.711.

4.2.4.2 Video Telephony (Optional)

The call control is performed in accordance with the SIP-Protocol as for Telephony, however specific options for multimedia communication are used.

For the Media-Stream the Codecs H.263 [29] and H.264 shall be used.

4.2.4.3 Fax and Modem

For Fax and Modem transmission over IP, ITU-T Rec. V.152 [33] (based on G.711a [26]) shall be used. If the adjacent endpoint does not support ITU-T Rec. V.152 [33], Fax- and Modem connections shall be set up using G.711a (ITU-T Rec. T.30 [31]).

For IMS UE to IMS UE communication the negotiation of T.38 regarding ITU-T Rec. T.38 (Edition 7) [32] is supported by the IMS platform of Deutsche Telekom. The Deutsche Telekom IMS is transparent for negotiation and transparent. An interworking of T.38 [2] towards PSTN is not supported. Interconnection with other carriers and mobile networks is dependent on the support of T.38 [32] in their network.

Only T.38 over UDPTL shall be supported.

Note: T.38 over UDPTL media encryption is not supported.

It is strongly recommended to implement the following codec negotiation scheme.

1. The originating UE (A-Side) send an initial INVITE with G.711 Faxcall towards the B-Side.
2. UE (B-Side) answers with 180 RINGING/200 OK INVITE.
3. Upon detection of facsimile by the receiving UE (B-Side), a SIP RE-INVITE request is sent to the originating UE (A-Side) of the initial INVITE (with the same Call-ID as the existing voice connection) for an ITU-T T.38 facsimile connection.
4. In cases where the UE (A-Side) which has sent the initial INVITE is not supporting T.38 a 488 shall be sent. However, the use of T.38 of the RE-INVITE does not cause the existing call to fail - the session continues using the previously negotiated characteristics. i.e Fax call using G.711.

Deutsche Telekom is not responsible for non-successful negotiation of T.38 regarding incompatible T.38 implementations. The procedure above allows the fall back to G.711 Fax.T.38 only negotiation may break.

Therefore, it is recommended that T.38 implementations support at minimum ITU-T Rec. T.38 Edition 7 to avoid interoperability problems with other T.38 implementations.

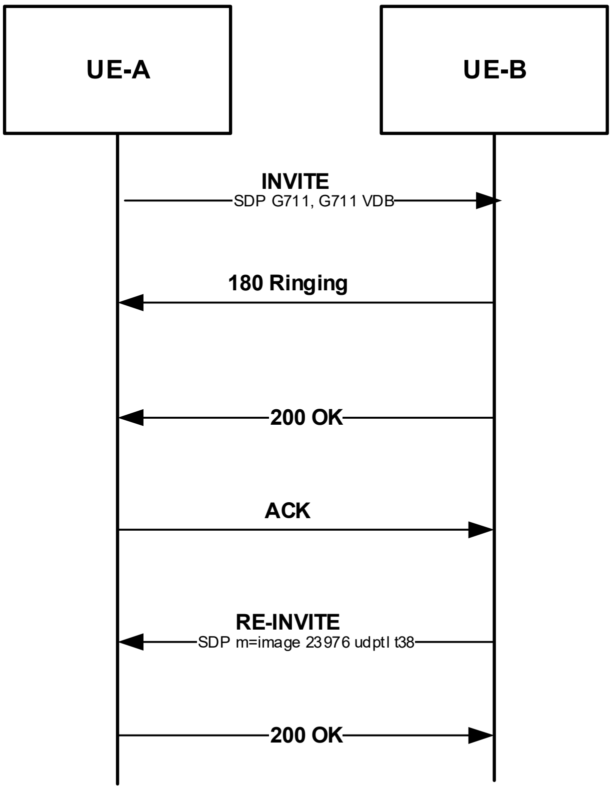
Further information about the support of T.38 in the IMS network of Deutsche Telekom is given under the following web address:

www.telekom.de/sonderdienste

Example of SDP sent within the RE-INVITE:

```
=== Session Description Protocol ===
Session Owner/Creator and session id : o=- 903412787 208218615 IN IP4 217.0.23.102
Media Name                           : m=image 23976 udptl t38
```

4.2.4.3.1 Callflow T.38 (informative)



4.2.4.4 DTMF

For DTMF events RFC 4733 [65] and RFC 5244 [67] shall be supported.

For support of DTMF RTP Out-of-Band in binary format RFC 4733 [65] and RFC 4734 [67] shall be supported.

> NOTE: In cases where the remote Endpoint does not support RFC4733 [65] it shall be possible to send DTMF inband.

It is recommended that DTMF applications always listen for Inband tones, even when DTMF events according to RFC 4733 and RFC 5244 were successful negotiated in the Offer/Answer procedure.

4.2.5 Reliability of provisional Responses

The support of Reliable Provisional Responses as defined in RFC3262 [27] and within 1TR114 (including Annex B) are mandatory. The following description shows the most important settings of the option tag 100rel and the procedures for sending PRACK/200 OK (PRACK):

1. RFC3262 [27] describes the procedures for the 100rel option tag: This option tag is for reliability of provisional responses. When present in a Supported header, it indicates that the UA can send or receive reliable provisional responses. When present in a Require header in a request, it indicates that the UAS MUST send all provisional responses reliably. When present in a Require header in a reliable provisional response, it indicates that the response is to be sent reliably.
2. The originating UE (UAC) shall include the 100rel option tag into the SIP supported header field of the INVITE as defined in RFC3262 [27].
3. Each INVITE received by a terminating UE (UAS) with a 100rel option tag in the SIP supported header indicates that the originating UE (UAC) is able to handle 100rel. In case the terminating UE (UAS) wants to have the provisional response reliable then it has to set the option tag 100rel in the require header as

defined in RFC3262 [27]. This is only allowed when the SDP answer contains the SDP to be used for the session.

4. Each Response received by the originating UE (UAC) with a 100rel in the required header shall be correctly answered regarding the procedures of 1TR114 and RFC3262 [27]. (i.e. sending PRACK)

NOTE: In case where the answer was sent in a reliable response the UE can receive a further offer within the PRACK. This offer is then answered within the 200 OK PRACK. UE's receiving the answer within a reliable response are using the UPDATE for sending an offer within the early dialog phase.

4.2.6 Early Media and Early Dialogs

4.2.6.1 General

Any final response either 200 OK or final error response (e.g. 4xx) as well as 199 shall close all existing early dialogs for the regarding Call-ID.

The AS sends a 199 for the release of early dialogs. A further 18x response (e.g. 180 in case of CCNR activation rejection) may be sent afterwards. For UE 199 is mandatory to understand.

4.2.6.1 Requirements

IAD-1	<u>Requirement Early-Media-Control</u> During early dialog phase the IAD provides for the user either silence or local ringtone or media received from the network.
IAD-2	<u>Silence ...</u> ... must be provided when neither 180 (Ringing) has been received nor backward early media is currently authorized or received from network.
IAD-3	<u>Local ringtone ...</u> ... must be provided when 180 (Ringing) has been received, but no backward early media is currently authorized nor received from network.
IAD-4	<u>Network early media (received RTP)</u> ... must be provided when backward early media is authorized from network and currently received.
IAD-5	<u>Forward early media</u> If forward early media is currently authorized from the network, the IAD must pass media originated by the user to the network.
IAD-6	<u>Requirement Initial-Early-Media-Control</u> Initially the media control is taken by the first early dialog which provides • either 18x response with P-Early-Media header with any value • or 18x response with an SDP answer (Note: ensures backward compatibility, if remote side does not support P-Early-Media) • or 180 (Ringing). In advance to take over of media control by any dialog, the IAD will not render any media received from remote nor generate local media towards the user).
IAD-7	<u>Requirement Change-of-Early-Media-Control</u>

<table>
<tr><td></td><td>The media control changes

a to another early dialog, if this other early dialog provides P-Early-Media=sendonly or sendrecv, or
b to any early dialog, if the early dialog which currently owns the media control terminates (199 (Early Dialog Terminated)). Hereby it is preferred to switch to the last dialog which provided media control, or
c to another dialog, if this other dialog provides an SDP answer for the first time and has not provided any P-Early-Media header in parallel or in any previous message (due to compatibility reasons a response, which provides initially an SDP answer but no P-Early-Media header, is treated per default as “P-Early-Media=sendonly”)
d to another early dialog, if current status is silence and 180 (Ringing) is received for this other dialog</td></tr>
<tr><td>IAD-8</td><td><u>Requirement Media-Sniffing (detection of RTP) shall be supported by the IAD</u>

If the dialog which owns the media control

• is in alerting phase (180 (Ringing) received for the given dialog)
• and P-Early-Media/SDP status of the dialog result in rendering of media from the network,
• but no RTP is received
then the IAD shall provide a local ringtone.

IAD shall observe RTP for 500ms to identify if RTP is received. If within 500 ms no RTP is received then the condition "no RTP" is fulfilled</td></tr>
<tr><td>IAD-9</td><td><u>Requirement Media-Behaviour:</u>

The IAD shall provide media according to the instructions received from the dialog which owns the media control as follows:

<table>
<tr><th colspan="4">dialog with media control:</th><th rowspan="2">resulting IAD behaviour</th></tr>
<tr><th>last P-Early-Media with direction attribute received for given dialog</th><th>SDP already received for given dialog</th><th>180 (Ringing) already received for given dialog</th><th>RTP received</th></tr>
<tr><td>none</td><td>no</td><td>no</td><td>n/a</td><td>silence</td></tr>
<tr><td>none</td><td>no</td><td>yes</td><td>n/a</td><td>local ringtone</td></tr>
<tr><td>none</td><td>yes1)</td><td>no</td><td>no</td><td>silence</td></tr>
<tr><td>none</td><td>yes1)</td><td>no</td><td>yes</td><td>render media received from network</td></tr>
<tr><td>none</td><td>yes1)</td><td>yes</td><td>no</td><td>local ringtone</td></tr>
<tr><td>none</td><td>yes1)</td><td>yes</td><td>yes</td><td>render media received from network</td></tr>
<tr><td>sendonly, sendrecv</td><td>no</td><td>no</td><td>n/a</td><td>silence</td></tr>
<tr><td>sendonly, sendrecv</td><td>no</td><td>yes</td><td>n/a</td><td>local ringtone</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>sendonly, sendrecv</td><td>yes</td><td>no</td><td>no</td><td>silence</td></tr>
<tr><td>sendonly, sendrecv</td><td>yes</td><td>yes[2)]</td><td>no[2)]</td><td>local ringtone</td></tr>
<tr><td>sendonly, sendrecv</td><td>yes</td><td>no/yes</td><td>/yes[2)]</td><td>render media received from network</td></tr>
<tr><td>inactive, recvonly</td><td>no/yes</td><td>no</td><td>no/yes</td><td>silence</td></tr>
<tr><td>inactive, recvonly</td><td>no/yes</td><td>yes</td><td>no/yes</td><td>local ringtone</td></tr>
</table>

<u>Notes:</u>
1) receipt of SDP w/o P-Early-Media: P-Early-Media is implicitly treated as sendonly (default)
2) immediately with receipt of P-Early-Media=sendonly/sendrecv any media received from the network shall be rendered. If sniffing timer (see. IAD-8) expires and 180 (Ringing) has been received and no RTP is received, then the IAD shall change to "local ringtone" (first row).
</td></tr>
<tr><td>IAD-10</td><td><u>Requirement P-Early-Media Support</u>

Support of P-Early-Media Header regarding RFC 5009 [109] is mandatory</td></tr>
</table>

4.2.6.2 Support of Specifications

The IETF RFC 5009 [109] and RFC 6228 [142] shall be supported.

NOTE: RFC 5009 [109] describes that the P-Early-Media header field in any message within an early dialog towards the sender of the INVITE request may contain the non-direction parameter "gated" to indicate that a network entity on the path towards the UAS is already gating the early media, according to the direction parameter(s). When included in the P-Early-Media header field, the "gated" parameter will come after all direction parameters in the parameter list. This parameter has no significant relevance for the UE.

4.2.6.3 Early media procedures

A VGW-A/IAD receiving the first provisional response received after sending INVITE shall evaluate SDP, P-Early-Media header filed and if RTP is received. The procedures shown in Figure G.2.1.1 Annex G must apply.

NOTE: SDP received by a UAC during an early dialog does not serve as an indication that early media will be received. Thus an IAD MUST support the detection of RTP received for that cases where the P-Early-Media header is not supported by the entity/network providing early media. (see also IAD-8, IAD-9)

When the terminating side is providing forking or features like forwarding or parallel ringing then multiple provisional responses may be sent back on separate early dialogs. Also other messages like an upstream SIP UPDATE request can update the early media state.

Depending on the State regarding Figure G.2.2.1 Annex G the succeeding received provisional responses must processed differently. Figure G.2.4.1 Annex G applies when Media (no ringback tone) is rendered to the user, Figure G.2.3.1 Annex G apply when further responses are needed to process the early dialog. Figure G.2.4.1 Annex G apply when a local ringback tone is played to the user.

When receiving provisional responses with a P-Early-Media header set to (sendonly or sendrecv) than the related early dialog shall take precedence as described in the Figures 14 Annex G -

All provisional responses shall be stored.

When a 199 (Early Dialog Terminated) response is received for an active early dialog then it shall be terminated. A RTP stream received associated with this particular early dialog shall no longer be rendered to the user. If the terminated dialog is the active one then the preceding early dialog stored by the IAD shall take precedence as described in Figure 1 in Annex G

The procedure shown in the Figures 1. to 4. shown in Annex G must apply

4.2.7 Registration & Authorization Procedures

4.2.7.0 General

UE shall minimise or avoid REGISTER procedures for identifying fetch bindings. The avoidance of this procedure is preferred to minimise the network load.

4.2.7.1 Support of Nonce for Authorization purposes

In general the nonce generated by the network is valid for "Authorization" as well as for "Proxy-Authorization".

The SIP www-authenticate and the Authorization header field is used for registering and re-registering the UE at the IMS. This is independent of the method used for registration.

The SIP Authentication-Info header field is used for providing the next-nonce in a 200 OK (REGISTER or INVITE)

Proxy- Authorization is used within INVITE containing the valid nonce to avoid a challenge response (i.e. 407)

4.2.7.2 Locating of P-CSCF (Proxy) in case of (re-) Registration and change of P-CSCF priority due to Maintenance

DNS SRV capabilities (including TTL) shall be supported (e.g. see chapter 4.2 in Annex B).

For P-CSCF discovery and Registration Procedures the Specifications TS 24.229 [21], RFC3261 [71], RFC 2782 [47] and RFC 3263 [50] are valid.

The following procedures shall give a hint for End device vendors how to implement these procedures to fulfil the requirements of Deutsche Telekom.

Due to maintenance and failure situations the prioritization of P-CSCF can change. Therefore the destination must be determined by applying the DNS procedures described within RFC3261 [71], RFC 2782 [47], RFC 3263 [50] and ANNEX B of this document.

In cases where the registration timer expires, or a network initiated deregister was sent or in cases where final responses where received pointing to a failure situation where the target cannot be reached (e.G. 503 Response) or a redirect (305 response) was received. A DNS query to request the actual SRV record set shall be done before sending a REGISTER or re-REGISTER request.

Only requesting a records is not allowed.

As described within RFC 2782 [47] a client MUST attempt to contact the target host (P-CSCF) with the lowest-numbered priority it can reach; target hosts with the same priority SHOULD be tried in an order defined by the weight field. Within Deutsche Telekom network normally only the priority field is used.

TTL expiry shall be taken into consideration when starting Register and re-Register procedures.

NOTE: A SIP UA stores the previously determined IP addresses, transport protocol and port of the P-CSCF for Register/Re-Register. In case resolution procedure fails the stored values are used. Stored value shall be overwritten with the actual values received by the DNS request. Stored value has a maximum lifetime of 4h.

4.2.7.3 SIP REGISTER Retry Mechanism in Failure Cases

4.2.7.3.1 General

This section is a General overview and extension of existing procedures within Annex B of this document and RFC 3261 and RFC 5626. This Overview overrules the text stated in Annex B (Sections 5.1.1 and 5.1.2.1).

4.2.7.3.2 Basic Guideline for re-transmissions of REGISTER requests is defined within RFC 3261.

RFC3261 defines the following timers:

```
Timer E initially T1    Section 17.1.2.2    non-INVITE request

                         retransmit interval,

                         UDP only
```

Note DT: Timer E is the retransmission timer. When timer E fires then the UA sends the request again. (retransmission of request)

```
Timer F 64*T1       Section 17.1.2.2    non-INVITE transaction

                         timeout timer
```

Note DT: When timer F fires then no response to one of the previous sent request (including the retransmitted requests) was received by the UA

```
RFC3261 Section 17.1.2.2 Formal Description

  The state machine for the non-INVITE client transaction is shown in
  Figure 6. It is very similar to the state machine for INVITE.

  The "Trying" state is entered when the TU initiates a new client
  transaction with a request. When entering this state, the client
  transaction SHOULD set timer F to fire in 64*T1 seconds. The request
  MUST be passed to the transport layer for transmission. If an
  unreliable transport is in use, the client transaction MUST set timer
  E to fire in T1 seconds. If timer E fires while still in this state,
  the timer is reset, but this time with a value of MIN(2*T1, T2).
  When the timer fires again, it is reset to a MIN(4*T1, T2). This
  process continues so that retransmissions occur with an exponentially
  increasing interval that caps at T2. The default value of T2 is 4s,
  and it represents the amount of time a non-INVITE server transaction
  will take to respond to a request, if it does not respond
  immediately. For the default values of T1 and T2, this results in
  intervals of 500 ms, 1 s, 2 s, 4 s, 4 s, 4 s, etc.
```

4.2.7.3.3 For 1TR114 implementation the following procedures shall apply when nor response is received for a REGISTER Request

Apply procedures for timer E and timer F as described within RFC 3261.

NOTE 1: Timer F runs and has a value of 32sec when T1 is set to default (500ms) i.e. a Request was already 10 times sent and no answer was received before timer F fires.

When timer F fires (no response received) then select a different P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in section 4.2.7.3 in this document and subclause 9.2.1 of 1TR114 Annex B (hint: SRV record). The next Register request shall be sent to the now selected P-CSCF.

NOTE 2: This was delivered via SRV records when requesting the DNS for P-CSCF addresses. As a minimum two addresses are delivered by the DNS. (see also Section 4.2.7.3 in this document [1TR114])

NOTE 3: It is a normal procedure of the DT end devices to request the DNS (under consideration of the TTL) before sending REGISTER requests (see also Section 4.2.7.3 in this document [1TR114]).

Proceed with: Subclause "4.2.7.3.5 Procedures after a minimum of 2 consecutive unsuccessful initial registration attempts."

4.2.7.3.4 For 1TR114 implementation the following procedures shall apply when an unsuccessful response is received for a REGISTER Request

For Failure Cases where SIP Requests are answered with 408 (Request Timeout) response or 500 (Server Internal Error) response or 503 (Service Unavailable) response or 504 (Server Time-Out) response or 600 (Busy Everywhere) response the following procedures shall apply:

If the retry after header is included then:

The UE shall attempt to perform initial registration after the value given within the retry after header. A different P-CSCF address from the list of P-CSCF addresses shall not be used.

If the retry after header is not included then:

1. The UE shall attempt to perform initial registration after 15 sec.
2. After a consecutive unsuccessful initial registration attempt then select a different P-CSCF address from the list of P-CSCF addresses discovered during the procedures described in subclause 9.2.1 of 1TR114 Annex B (SRV record), and
3. The UE shall attempt to perform initial registration to the now selected P-CSCF.
4. After a consecutive unsuccessful initial registration attempt then the UE shall attempt to perform initial registration either after the value given within the retry after header or after 15 sec.
5. If the selected P-CSCF address was the last address resolved then proceed with step 6. If a further P-CSCF address is available then proceed with step 2.
5. After 2 consecutive unsuccessful initial registration proceed with: Subclause "4.2.7.3.5 Procedures after a minimum of 2 consecutive unsuccessful initial registration attempts".

4.2.7.3.5 Procedures after a minimum of 2 consecutive unsuccessful initial registration attempts

NOTE: This is valid for REGISTER requests either receiving an unsuccessful response or no response.

After a minimum of 2 consecutive unsuccessful initial registration attempts, the UE shall implement the mechanism defined in subclause 4.5 of RFC 5626 [68] for new registration attempts. The UE shall use the values of the parameters max-time and base-time, of the algorithm defined in subclause 4.5 of RFC 5626 [68]. If no values of the parameters max-time and base-time have been provided to the UE by the network, the default values defined in in subclause 4.5 of RFC 5626 [68] shall be used.

The values of max-time and base-time may be provided by the network to the UE using OMA-DM with the management objects specified in 3GPP TS 24.167 [8G]. Other mechanisms may be used as well and are outside the scope of the present specification.

RFC 5626 [68] Section 4.5 is valid as follows:

```
RFC5626 Section 4.5. Flow Recovery
```

When a flow used for registration (through a particular URI in the outbound-proxy-set) fails, the UA needs to form a new flow to replace the old flow and replace any registrations that were previously sent over this flow. Each new registration MUST have the same reg-id value as the registration it replaces. This is done in much the same way as forming a brand new flow as described in Section 4.2; however, if there is a failure in forming this flow, the UA needs to wait a certain amount of time before retrying to form a flow to this particular next hop.

The amount of time to wait depends if the previous attempt at establishing a flow was successful. For the purposes of this section, a flow is considered successful if outbound registration succeeded, and if keep-alives are in use on this flow, at least one subsequent keep-alive response was received.

The number of seconds to wait is computed in the following way. If all of the flows to every URI in the outbound proxy set have failed, the base-time is set to a lower value (with a default of 30 seconds); otherwise, in the case where at least one of the flows has not failed, the base-time is set to a higher value (with a default of 90 seconds). The upper-bound wait time (W) is computed by taking two raised to the power of the number of consecutive registration failures for that URI, and multiplying this by the base-time, up to a configurable maximum time (with a default of 1800 seconds).

W = min (max-time, (base-time * (2 ^ consecutive-failures)))

These times MAY be configurable in the UA (via TR-069 [72] Reference number out of 1 TR 114]). The three times are:

- max-time with a default of 1800 seconds
- base-time (if all failed) with a default of 30 seconds
- base-time (if all have not failed) with a default of 90 seconds

For example, if the base-time is 30 seconds, and there were three failures, then the upper-bound wait time is min(1800, 30*(2^3)) or 240 seconds. The actual amount of time the UA waits before retrying registration (the retry delay time) is computed by selecting a uniform random time between 50 and 100% of the upper-bound wait time. The UA MUST wait for at least the value of the retry delay time before trying another registration to form a new flow for that URI (a 503 response to an earlier failed registration attempt with a Retry- After header field value may cause the UA to wait longer).

To be explicitly clear on the boundary conditions: when the UA boots, it immediately tries to register. If this fails and no registration on other flows succeed, the first retry happens somewhere between 30 and 60 seconds after the failure of the first registration request. If the number of consecutive-failures is large enough that the maximum of 1800 seconds is reached, the UA will keep trying indefinitely with a random time of 15 to 30 minutes between each attempt.

4.2.7.3. Additional requirements for De-Registration

In cases where UEs are booting, there is no knowledge if the UE is already registered or not. Therefore, De-Register with "*" in the contact header field is forbidden and shall not be sent.

Network initiated De-Registration is part of this specification and must be supported.

4.2.7.4 Implicit Registration

Implicit Registration shall be supported with the following procedures:

For each stored Public URI’s (IMPU) received via TR-069 [72], TR-181 [74] and TR104 [72] protocol via the initial configuration the following registration procedure shall apply.

During the initial configuration with the TR-069 [72], TR-181 [74] and TR104 [72] protocol each received IMPU shall be stored.

For each IMPU an explicit registration shall apply with the following exception.

In cases where a P-Associated-URI with additional registered URI’s (implicit registration set) is received the IAD shall compare these URIs with the stored URI’s received via TR-069 [72], TR-181 [74] and TR104 [72].

For IMPU’s implicit registered an explicit registration shall not apply in addition.

4.2.7.5 Challenge for Registration and other SIP Messages

- The challenge mechanism shall be supported.

Note: This requirement seen from UE point of view is needed that a received 401 or 407 is processed properly. I.e. using the correct nonce and procedures as defined in RFC 2617 [21] and this document for the next request sent by the UE. This shall apply for NASS bundled as well as for Digest authentication.

- To avoid too many challenge cycles the nonce shall be included within each request during its validity.

Note: This requirement seen from UE point of view is needed to include the stored credentials (nonce value) into the next request. This shall apply for NASS bundled as well as for Digest authentication.

- The next-nonce mechanism as defined within RFC 2617 [21] and this document shall be supported.
- The nonce received in 401 or 407 by the UE is valid for registration as well as for initial requests.
- The next- nonce received in a 200 OK is valid for next requests (including REGISTER) sent by the UE.
- The latest receives “next-nonce” shall be used for the Re-REGISTER.

4.2.8 Secure VOIP

Key Negotiation Method SDES; 3DES(Session Description Protocol Security Descriptions for Media Streams) shall be supported.

IETF draft-dawes-dispatch-mediasec-parameter-08.txt "Security Mechanism Names for Media" [79] should be considered in addition.

Procedures described within 1 TR 114 ANNEX B are valid. The following text shows some parts of the valid text.

As shown in 1 TR 114 ANNEX B the UE behaviour is as follows:

To request end to access edge media security either on a session or media level, the UE shall send an SDP Offer for an SRTP stream containing one or more SDES crypto attributes, each with a key and other security context parameters required according to RFC 4568 [77], together with the attribute "a=3ge2ae:requested".

This attribute is supported in the IMS of Deutsche Telekom. The definition of this element is Annex B

General: end-to-end media security is NOT required, thus their procedures shall not be implemented.

For each TLS session of within one IAD, a krypto key is needed.

So for each additional dialog a new krypto key is needed.

e.g. 2 TLS Session = 2 krypto keys used = 2 SRTP sessions

4.2.8.1 Cipher Suites:

PFS (Perfect Forward Secrecy) Cipher Suites should be used only. Cipher suits define the "Key-negotiation" and "Key agreement" (and Authentication if needed), media encryption and a hash functionality for integrity protection (HAMAC-Algorithm) and use for the pseudorandom function starting with TLS 1.2.

A full list of all defined Cipher-Suites including references to the regarding specifications is given under http://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml.

Table 3.2-1 shows the Cipher Suits required for Deutsche Telekom Client implementation. In brackets the OpenSSL equivalents are shown. The UE (IAD) shall support at minimum one of the following Cipher suits using TLSv1.2.

The cipher suit number 1 and 2 out of Table 4.2.8.1 -1 SHALL be implemented, the cipher suit offer shall have the sequence as shown within Table 4.2.8.1 -1.

Table 4.2.8.1 -1: Supported Cipher Suites

Number	Cipher Suite	TLS	Reference	Support in UA (NOTE 1)
1	TLS_AES_128_GCM_SHA256	TLSv1.3	RFC8446 [201]	m
2	TLS_AES_256_GCM_SHA384	TLSv1.3	RFC8446 [201]	m
3	TLS_AES_128_CCM_SHA256	TLSv1.3	RFC8446 [201]	m
4	TLS_CHACHA20_POLY1305_SHA256	TLSv1.3	RFC8446 [201]	m
5	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (ECDHE-RSA-AES256-GCM-SHA384)	TLSv1.2	RFC5289 [87]	m
6	TLS_RSA_WITH_AES_256_GCM_SHA384 (AES256-GCM-SHA384)	TLSv1.2	RFC5288 [89]	o
7	TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (ECDH-RSA-AES256-GCM-SHA384)	TLSv1.2	RFC5289 [87]	o
8	TLS_RSA_WITH_AES_256_CBC_SHA256 (AES256-SHA256)	TLSv1.2	RFC5288 [89]	o
9	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (ECDHE-RSA-AES128-GCM-SHA256)	TLSv1.2	RFC5289 [87]	o (NOTE 3)
10	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (ECDHE-RSA-AES128-SHA256)	TLSv1.2	RFC5289 [87]	o (NOTE 2)
11	TLS_RSA_WITH_AES_128_GCM_SHA256 (AES128-GCM-SHA256)	TLSv1.2	RFC5246 [88]	o (NOTE 4)
12	TLS_RSA_WITH_AES_128_CBC_SHA256 (AES128-SHA256)	TLSv1.2	RFC5246 [88]	o (NOTE 4)
NOTE 1: At minimum one of the TLSv1.2 and TLS 1.3 shown cipher suites shall be supported. Priority of implementation starts on top of the table. NOTE 2: An elliptical cipher suite shall be implemented in addition if the non elliptical Cipher suite regarding RFC 5246 [88] is implemented. NOTE 3: Mandatory for UE/IAD supporting SIP-Trunk (i.e SIP Connect 2.0) NOTE 4: Optional support for UE/IAD supporting SIP-Trunk (i.e SIP Connect 2.0) (for backward compatibility)				

4.2.8.2 Key Size / Key Length

It is recommended to use the following Key Length:

Table 4.2.8.2-1: Supported Algorithms in UA

Algorithm	Minimal Key Length	Recommended use till year	Support in UA
Digital Signature Algorithm and key negotiation			

ECDSA	250 Bit (NOTE 5)	2027	m
DSS	2000 Bit (NOTE 6)	2022	m
DSS	3000 Bit (NOTE 6)	2027+	m
RSA	2000 Bit (NOTE 6)	2023	m
RSA	3000 Bit (NOTE 6)	2027+	m
Static Diffie-Hellman Key			
ECDH	250 Bit (NOTE 5)	2027+	o
DH	2000 Bit (NOTE 6)	2022	o
DH	2000 Bit (NOTE 6)	2027+	o
Ephemerale Diffie-Hellman Key			
ECDH	250 Bit (NOTE 5)	2027+	m
DH	2000 Bit (NOTE 6)	2022	m
DH	3000 Bit (NOTE 6)	2027+	m
NOTE 5: In this case 250 Bit (instead of 256 Bit) are used to allow small Co-Factors at elliptical curves. NOTE 6: For use beyond 202 it is useful to use RSA/DSS/DH-Key of 3000 Bit length to ensure a consistent security level of all recommended asymmetric encryption methods.			

Session renegotiation based on RFC5746 [86] shall be implemented.

Client based Session Renegotiation must be rejected.

It is not needed to support the TLS 1.2 extension "truncated_hmac" as defined in RFC6066 [85].

An implementation of TLS-Compression as defined in TLS 1.2 RFC 5246 [42] is not needed.

4.2.8.3 Algorithms for Elliptic Curve Cryptography

Elliptical curves recommended in chapter 3.6 of BSI TR-02102-2 [80] shall be supported as follows.

Table 4.2.8.3-1: Supported Elliptic Curve in UA

Curve	Specification and Reference	Support in UE
brainpoolP256r1	RFC5639 [83] and RFC7027 [84]):	m
brainpoolP384r1	RFC5639 [83] and RFC7027 [84]):	m
brainpoolP512r1	RFC5639 [83] and RFC7027 [84]):	m
secp224r1	SECG Standards; www.secg.org	o
secp256r1	SECG Standards; www.secg.org	o
secp384r1	SECG Standards; www.secg.org	o

4.2.8.4 Root Certificate

4.2.8.4.1 Initial

The UE MUST comply to X.509v3 acc. RFC 5280 [93].

The device MUST comply to industry standard guidelines related to security handling/administration as well as to the requirements of Deutsche Telekom like particularly " Security Requirement Home Gateway" (see chapter 'References').

The UE MUST store all Certificate Authority (CA) Information Chain according X.509v3 to ensure that a requestor (SIP client) is able to validate the Certificate.

The HG must be able to cope with a chain of trust depth of >2.

4.2.8.4.2 Update

The UE MUST provide the ability to update the root certificates by new Firmware update (regardless if locally or remotely initiated).
The secure connections described within this document are solely established to the trusted Telekom platform only, therefore as a matter of fact there seems to be no need for further manual update procedures for the moment.

4.2.8.4.3 Deutsche Telekom Certificate download

End-devices (UE) must install locally the certificate of Telesec Root-CA (manually) or it is pre-installed by the vendor of the corresponding operating system / SIP software.

The certificate is **T-TeleSec GlobalRoot Class 2** with fingerprint 590d2d7d884f402e617ea562321765cf17d894e9

https://www.telesec.de/de/root-programm/informationen-zu-ca-zertifikaten/root-ca-zertifikate/

This link is subject to change by Telesec.

Note, depending on that certificate been used, only Telesec Root Certificate is required.

UE must check the validity of the certificate provided by P-CSCF/IBCF with help of root certificate.

4.2.8.6 SRTP Profile

§Annex C (Normative) out of 3GPP TS 33.328 [19C] Release 12: SRTP profiling for IMS media plane security

An IMS UE and IMS core network entity capable of supporting IMS media plane security (SDES and/or KMS based)

- Shall support all mandatory features defined in RFC 3711 [9] except that it does not have to support key derivation rates different from zero (KDR <> 0).

- May support RFC 4771, "Integrity Transform Carrying Roll-Over Counter for the Secure Real-time Transport Protocol (SRTP)" [RFC 4771] for SDES based media plane security. RFC 4771 shall be supported and used for KMS based media plane security RFC 4771 defines functionality that is essential to simplify late entry in group communications and broadcasting sessions.

NOTE: Media security context update is not used with e2ae security.

4.2.8.7 Profiling of SDES

§Annex E (normative):out of 3GPP TS 33.328 [19C] Release 12 Profiling of SDES

The present Annex contains a complete list of parameters that may be contained in an SDES crypto attribute, according to RFC 4568.

The following short-hand notation is used:
- “mandatory / optional to support / use” means: “This parameter shall / may be supported / used in implementations conforming to 3GPP specifications.”

The default use is that the sender omits the parameters that are optional to use.

CRYPTOGRAPHIC ALGORITHMS

cryptosuite: mandatory to support and use

In addition to mandating the support and use of the parameter “cryptosuite” in an SDES crypto attribute, the cryptosuite “AES_CM_128_HMAC_SHA1_80”, as defined in RFC 4568, is mandatory to support.

"KEY PARAMETERS" (ONE OR MORE TIMES):

key: mandatory to support and use

salt: mandatory to support and use

key lifetime: optional to support and use for e2e security, shall not be used for e2ae security (cf. clauses 7.2.1 and 7.3.1 of this specification).

Master Key Index (MKI): optional to support, mandatory to use if more than one set of key parameters is contained in the crypto attribute, otherwise optional to use. If only one master key is used, an MKI is not recommended to be used.

NOTE: It is not guaranteed that implementations support more than one master key per crypto attribute. If only one master key is used, an MKI has no function as it adds to the SRT(C)P packet overhead.

Length of MKI field: optional to support, mandatory to support if MKI is supported, mandatory to use if MKI is used.

"SESSION PARAMETERS"

key derivation rate: optional to support and use

UNENCRYPTED_SRTP: mandatory to support and optional to use

UNENCRYPTED_SRTCP: mandatory to support and optional to use

UNAUTHENTICATED_SRTP: mandatory to support and optional to use

NOTE: The flags “UNENCRYPTED_SRTP” and “UNENCRYPTED_SRTCP**”** may be useful when regulations do not permit encryption, but authentication is still desired. The flag “UNAUTHENTICATED_SRTP” may be useful to reduce the packet size for e.g. voice traffic where integrity protection may not be needed, cf. the situation on 3GPP radio interfaces over which user data are not integrity-protected.

forward error correction order: not applicable

key parameters for the FEC stream: optional to support and use

window size hint: optional to support and use

Deutsche Telekom endorsement, the following parameter settings shall be used:

Parameter	***Default***
Key derivation rate	***0***
Master key length	***128 bits***
Master salt key length	***112 bits***
PRF	***AES_CM***
Session authentication key length	***128***

Parameter	***Default***
Session encryption key length	***128 bits***
Session salt key length	***112***
SRTP authentication	***HMAC-SHA1***
SRTCP authentication	***HMAC-SHA1***
SRTP HMAC tag length	***80***
SRTCP HMAC tag length	***80***
SRTP packets maximum lifetime	***2^48 packets***
SRTCP packets maximum lifetime	***2^31 packets***
SRTP replay-window size	***64***
SRTCP replay-window size	***64***

4.2.9 GRUU (Optional)

The GRUU functionality is mainly used for the Deutsche Telekom Product DIPVD (DeutschlandLAN IP Voice/Data) to allow small PBX up to 8 active calls plus 8 calls on HOLD.

The following figure shows a possible implementation of an IAD:

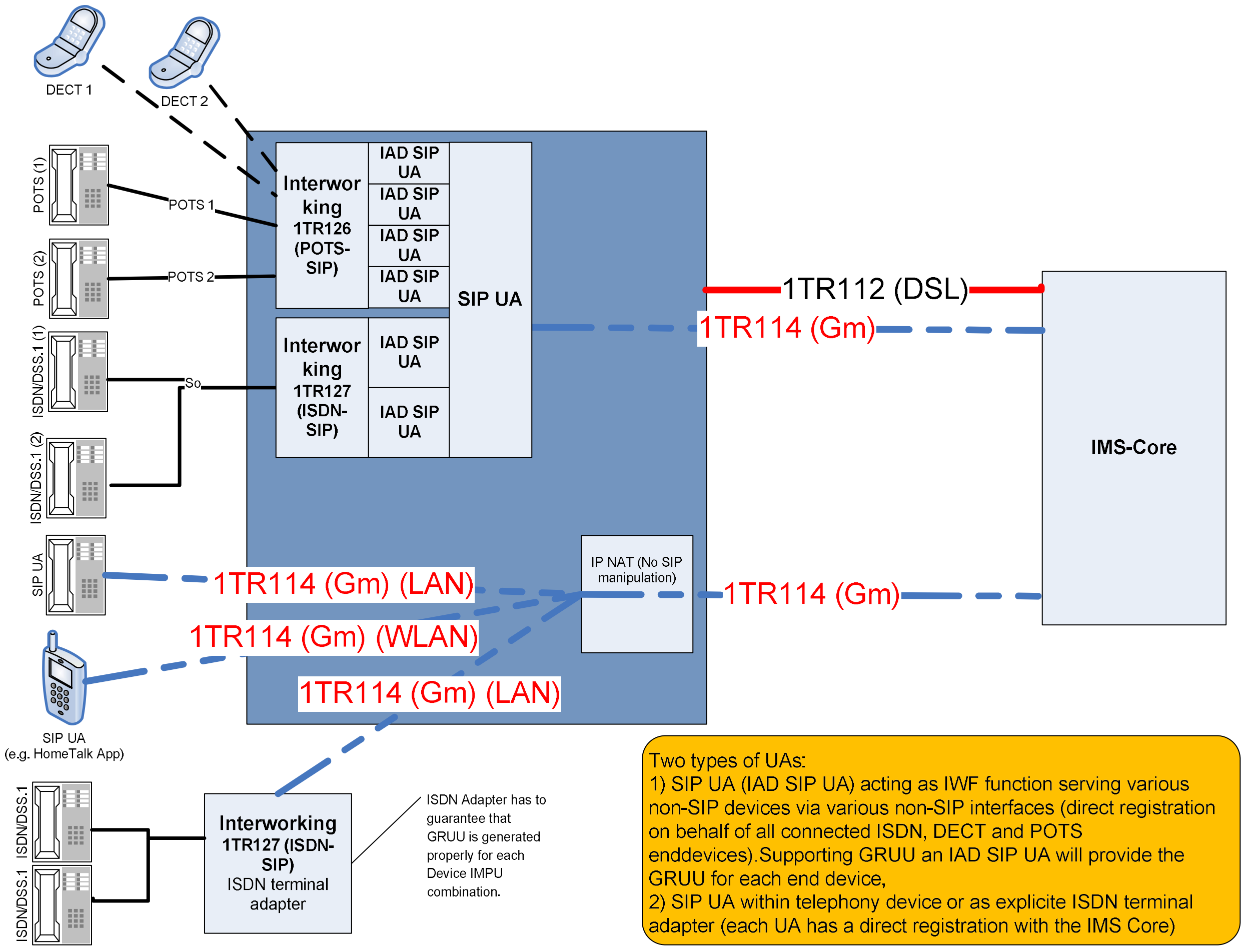


Figure 1 Possible architecture of an IAD with support of GRUU

For each IAD SIP UA the following procedures SHALL apply:

– Create a unique identifier (GRUU) for each IAD SIP UA,
– Depended on implementation SIP UA shall act as a registrar. It shall accept REGISTER from IAD SIP UA and create a unique identifier for each binding, or
– Generate for each IAD SIP UA a unique binding,
– For all requests and responses containing a SIP Contact header field (except REGISTER) sent by the SIP UA, the SIP UA shall add a GRUU to the SIP Contact header field based on the related IAD SIP UA.
– The Contact header with GRUU shall apply to the format as defined within RFC 5627 [69] as follows:
    - Contact: <contact-URI; gr=urn:uuid:random-string>
    - Example: Contact: <sip:iad-1@62.57.4.12; gr=kjh29x97us97d>
– The SIP UA shall extract telephone number from the P-Called-Party-Identity header and ring ports with matching configuration
– SIP UA shall create IMPU of configured telephone number and domain name and apply it to the P-Preferred-Identity and From headers

The GRUU shall be supported by the SIP Agents used within the IAD as follows.

Each IAD SIP UA shall have an internally registered GRUU as defined within RFC 5627 [69] which shall be populated within each contact of non-REGISTER requests and its responses. The use of Session-ID as defined in RFC 5626 [68] SHALL NOT apply.

The following procedure for constructing a self-made GRUU in RFC5627 [69] section 4.3 shall apply

- A self-made GRUU is one whose domain part equals the IP address or hostname of the user agent. The user part of the SIP URI is chosen arbitrarily by the user agent. Like all other GRUUs, the URI MUST contain the "gr" URI parameter, with or without a value, indicating it is a GRUU.

  Example: sip:alice@example.com;gr=kjh29x97us97d✓

As defined in RFC 5627 [69] the SIP UA shall us its own GRUUs as defined in Section 4.4 “Using One's Own GRUUs” of RFC5627 [69] as follows:

> A SIP UA SHOULD use a GRUU when populating the Contact header field of dialog-forming and target refresh requests and responses. In other words, a UA compliant to this specification SHOULD use one of its GRUUs as its remote target. This includes:
>
> - the INVITE request
> - a 2xx or 18x response to an INVITE which contains a To tag,
> - the UPDATE request
> - a 2xx response to an UPDATE

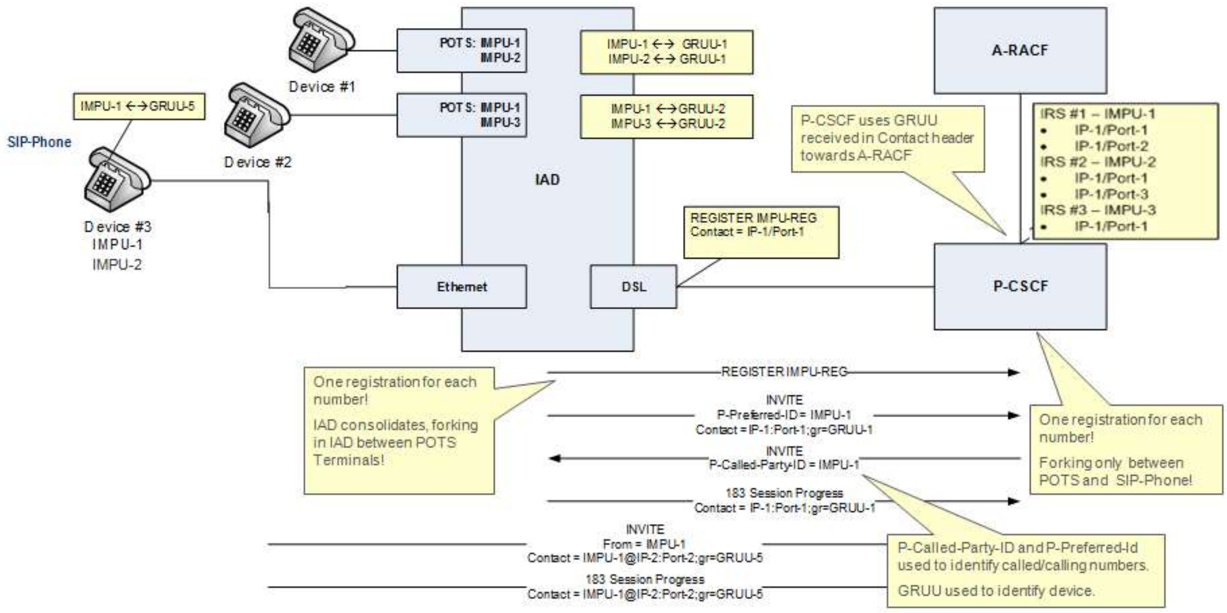


Figure 2 Principle of GRUU in SIP Messages

NOTE: The implementation of GRUU is not relevant for implementations according to 1TR118 [91] / 1TR119 [92]

4.2.10 Reliable SIP & RTP Processing

The device shall support Reliable SIP request processing to be robust and Reliable against SIP attacks, e.g. SIP vicious.

The device shall only process SIP requests, received on its WAN interface, from P-CSCF source IPs (IPv4 or IPv6) which the Telekom VoIP account of the device is successfully registered to.

NOTE: The P-CSCF is the Deutsche Telekom IMS entity equivalent with a outbound proxy defined within SIP RFC 3261. The Deutsche Telekom used entity follows the 3GPP and ETSI TISPAN specifications. The needed UE procedures are defined within the main 1TR114 document.

In addition, the device shall handle multiple registered conditions in edge scenarios, to process SIP requests from P-CSCF source

IPs (IPv4 or IPv6), e.g. due to synchronization time offset:

1. Telekom VoIP account X is registered to P-CSCF 1

1.1 Telekom VoIP account Y is registered to P-CSCF 1

1.2 Re-Register process for Telekom VoIP Account Y is succeeded to P-CSCF 1

1.3 Re-Register process for Telekom VoIP account X is not possible to P-CSCF 1(P-CSCF 1 is temporarily unavailable), Telekom VoIP account X is then re-registering to P-CSCF 2 and also still registered to P-CSCF 1 until the valid register to P-CSCF 1 is expired.

In that case the VoIP account X is still registered to P-CSCF 1 and registered to P-CSCF 2

Additionally, all P-CSCF source IPs (IPv4 or IPv6) which are successfully resolved, based on device DNS resolution e.g. via SRV / AAAA / A records, are valid for P-CSCF source IP request processing. (under consideration of the TTL).

The device shall process SIP requests from SIP UA within the Home Network without any malfunction.

The device shall support Reliable SIP request processing with all valid SIP request methods acc. to RFC 3261, RFC 3262, RFC 6665, RFC 6086, RFC 3513, RFC 3311.

This P-CSCF origin based Reliable SIP request processing shall be valid for Telekom as VoIP provider.

4.2.12 Auto configuration

Auto configuration procedures are described within the Broadband Forum Technical Reports TR-069 [72], TR-181 [74] and TR104 [72] and shall be considered for the implementation.

4.2.13 Overlap Signalling

The use of overlap signalling as defined in 3GPP TS 24.229 [21] shall not be supported at the Gm interface. i.e. neither “multiples INVITES” nor the “in-dialog” method shall be used. Overlap dialling shall be converted within the UE to en-block (i.e. complete request URI). A dialled # should be interpreted as end of dialling.

Mechanisms to identify the end of dialling within the UE may be used like:

- Receipt of the maximum number of digits used in the national numbering plan.
- Analysis of called number based on an implemented directory.
- Analysis of called number based on already successful called numbers.

Adaptive inter-digit timer.

4.2.14 Preconditions

The support of preconditions is OPTIONAL. i.e Deutsche Telekom does not use preconditions in the IMS.

If the end device vendor decides to implement preconditions then the procedures shall be disabled.

The request of preconditions (indication of SUPPORT/REQUIRED) within an initial INVITE) with the initial INVITE SHALL NOT be done.

5 SIP Service functionality requirements

5.1 General

The SIP service functionality requirements are defined in Annex B of the present document.

6 Void

7 Protocol (Profiles)

This section profiles the Gm interface for SIP UE intended to be connected to the NGN platform of Deutsche Telekom based on 3GPP TS 24.229 Release 11 [21] (endorsements).

Markings general used within the TEXT:

Text modified due to Deutsche Telekom requirements that is added or deleted compared to 3GPP TS 24.229 Release 11 [21]is shown as cursive and underlined (*<u>example for added text</u>*) or cursive and stricken (*~~example for stricken text~~*).

For information: As usual within 3GPP Standards notes in Tables are mandatory and have to be implemented

7.1 Void

7.2 Modifications to 3GPP TS 24.229 (endorsement)

The relevant modifications to 3GPP TS 24.229 [21] for SIP UE (Gm interface) intended to be connected to the NGN platform of Deutsche Telekom are provided in Annex B of the present document.

7.3 UE (Gm) interface; Profile tables based on 3GPP TS 24.229

In the following section the actual numbering of the endorsement document is kept with a leading “§” sign, if applicable. If not explicit noted, the references mentioned within the following tables apply to Annex B **i.e the numbering of reference [xyz] is the same as used within TS 24.229** [21]. The Reference section is in ANNEX B Section 2

7.3.1 Table description

Table 7.3.1.1: Table Type 1 Example

Item	PDU or Header	Sending			Receiving		
		Ref.	Profile status UE	UNI (Gm)	Ref.	Profile status UE	UNI (Gm)
1	2	3	4	5	6	7	8

Legend:

Column 1: Item numbering

Column 2: Identification of PDU (Method) or SIP Header

Column 3/4/5: Sending = from UE to P-CSCF

Column 6/7/8: Receiving = from P-CSCF to UE

Column 3/6: Reference to section 2 "References" in Annex B .e the numbering of reference [xyz] is the same as used within TS 24.229 [21]. The Reference section is in ANNEX B Section 2

Column 4/7: Profile Status of capabilities the UE has to support

Column 5/8: Profile Status of the IMS Gm Interface

7.3.2 PDUs (SIP Methods)

The following methods shall be supported on the Gm Interface and the UE.

NOTE: A Method Request (e.g. INVITE request) is the Method itself. A Method Response is the Response (e.g. 1xx) sent as a result of a Request.

The following table is based on Table §A.5: "Supported methods" of Annex B and profiled for this document.

Table 7.3.2.1: Supported methods

Item	PDU	Sending			Receiving		
		Ref.	Profile status UE	UNI (Gm)	Ref.	Profile status UE	UNI (Gm)
1	ACK request	[26] 13	m	m	[26] 13	m	m
2	BYE request	[26] 15.1	m	m	[26] 15.1	m	m
3	BYE response	[26] 15.1	m	m	[26] 15.1	m	m
4	CANCEL request	[26] 9	m	m	[26] 9	m	m
5	CANCEL response	[26] 9	m	m	[26] 9	m	m
6	INFO request	[26] 13	c6	m	[26] 13	c5	m
7	INFO response	[26] 13	c6	m	[26] 13	c6	m
8	INVITE request	[26] 13	m	m	[26] 13	m	m

Item	PDU	Sending			Receiving		
		Ref.	Profile status UE	UNI (Gm)	Ref.	Profile status UE	UNI (Gm)
9	INVITE response	[26] 13	m	m	[26] 13	m	m
9A	MESSAGE request	[50] 4	c11	m	[50] 7	c10	m
9B	MESSAGE response	[50] 4	c11	m	[50] 7	c11	m
10	NOTIFY request	[28] 8.1.2	c8	m	[28] 8.1.2	c9	m
11	NOTIFY response	[28] 8.1.2	c8	m	[28] 8.1.2	c8	m
12	OPTIONS request	[26] 11	o	m	[26] 11	m (NOTE 1)	m
13	OPTIONS response	[26] 11	o	m	[26] 11	o	m
14	PRACK request	[27] 6	c7	m	[27] 6	c7	m
15	PRACK response	[27] 6	c7	m	[27] 6	c7	m
15A	PUBLISH request	[70] 3	c15	c15	[70] 3	c14	c14
15B	PUBLISH response	[70] 3	c15	c15	[70] 3	c15	c15
16	REFER request	[36] 3	c13	m	[36] 3	c12	m
17	REFER response	[36] 3	c13	m	[36] 3	c13	m
18	REGISTER request	[26] 10	c16	c16	[26] 10	n/a	n/a
19	REGISTER response	[26] 10	n/a	n/a	[26] 10	c16	c16
20	SUBSCRIBE request	[28] 8.1.1	m	m	[28] 8.1.1	o	m
21	SUBSCRIBE response	[28] 8.1.1	m	m	[28] 8.1.1	o	m
22	UPDATE request	[30] 6.1	m	m	[30] 6.2	m	m
23	UPDATE response	[30] 6.2	m	m	[30] 6.1	m	m
24	other requests		n/a	n/a		n/a	c3
25	other response		n/a	c2		n/a	n/a

Conditions for Table 7-1:

c1: IF received reject with 405.

c2: IF received then response shall be ignored.

c3: IF received reject with 501.

c4: Void.

c5: IF AoC or other Deutsche Telekom applications using INFO Then m ELSE c1.

c6: IF AoC or other Deutsche Telekom applications using INFO Then m ELSE n/a.

c7: IF preconditions or Tones and Announcements (early media) with 18x THEN m ELSE o.

c8: IF CCBS or Dial tone Package or other Deutsche Telekom applications using NOTIFY THEN m ELSE n/a.

c9: IF CCBS or Dial tone Package or other Deutsche Telekom applications using NOTIFY THEN m ELSE c1.

c10: needed for future services (please note that MWI is no longer supported within Deutsche Telekom Core Network).

c11: needed for future services (please note that MWI is no longer supported within Deutsche Telekom Core Network).

c12: IF ECT or other application using REFER message THEN m Else c1.

c13: IF ECT or other application using REFER message THEN m Else n/a.

c14: IF Presence or other application using Publish THEN m ELSE c1.

c15: IF Presence or other application using Publish THEN m ELSE n/a.

c16: IF A.4/1 in ANNEX B THEN m ELSE n/a - - client behaviour for registration.

c17 IF A.4/17 in ANNEX B THEN m ELSE n/a - - the SIP UPDATE method?

NOTE 1: The OPTION method is used to check reliability between UE and P-CSCF.

7.3.3 Supported status-codes on the Gm -Interface

See 1TR114 Annex B Table A.6

7.3.4 Support of SIP Headers on the UNI (Gm) -Interface

The information given within this section is a simplified presentation of the used headers.

The following SIP Headers shall be supported on the UNI (Gm) -Interface:

Table 7.3.4.1: Supported headers

Item	Header	Sending (UE to P-CSCF)			Receiving (P-CSCF to UE)		
		Ref.	Profile status UNI (Gm)	Profile status UE	Ref.	Profile status UNI (Gm)	Profile status UE
1	Accept	[26] 20.1	m	m	[26] 20.1	m	m
2	Accept-Contact	[56B] 9.2	o	o	[56B] 9.2	o	o
3	Accept-Encoding	[26] 20.2	o	o	[26] 20.2	o	o
4	Accept-Language	[26] 20.3	o	o	[26] 20.3	o	o
5	Alert-Info	[26] 20.4	o	m	[26] 20.4	o	m
6	Allow	[26] 20.5, [26] 5.1	m	m	[26] 20.5, [26] 5.1	m	m
7	Allow-Events	[28] 7.2.2	o	m	[28] 7.2.2	o	m
7b	Answer-Mode	[158]	o	o	[158]	o	o
8	Authentication-Info	[26] 20.6	o	m	[26] 20.6	o	m
9	Authorization	[26] 20.7	m	m	[26] 20.7	c2	c2
10	Call-ID	[26] 20.8	m	m	[26] 20.8	m	m
11	Call-Info	[26] 20.9	o	n/a	[26] 20.9	o	m
12	Contact	[26] 20.10	m	m	[26] 20.10	m	m
13	Content-Disposition	[26] 20.11	o	m	[26] 20.11	o	m
14	Content-Encoding	[26] 20.12	o	m	[26] 20.12	o	m
15	Content-Language	[26] 20.13	o	m	[26] 20.13	o	m
16	Content-Length	[26] 20.14	m	m	[26] 20.14	m	m
17	Content-Type	[26] 20.15	m	m	[26] 20.15	m	m
18	CSeq	[26] 20.16	m	m	[26] 20.16	m	m
19	Date	[26] 20.17	o	m	[26] 20.17	o	m
20	Error-Info	[26] 20.18	o	o	[26] 20.18	o	m
21	Event	[28] 8.2.1	o	m	[28] 8.2.1	o	m
22	Expires	[26] 20.19	o	m	[26] 20.19	o	m
23	From	[26] 20.20	m	m	[26] 20.20	m	m

Item	Header	Sending (UE to P-CSCF)			Receiving (P-CSCF to UE)		
		Ref.	Profile status UNI (Gm)	Profile status UE	Ref.	Profile status UNI (Gm)	Profile status UE
23A	Geolocation	[89] 3.2	o	o	[89] 3.2	o	o
23B	Geolocation-Routing	[89] 4.2	o	o	[89] 4.2	o	o
24	History-Info	[66] 4.1	n/a	n/a	[66] 4.1	o	m
25	In-Reply-To	[26] 20.21	o	o	[26] 20.21	o	o
26	Join	[61] 7.1	o	o	[61] 7.1	o	o
26b	Max-Breadth	[117]	o	o	[117]	n/a	n/a
27	Max-Forwards	[26] 20.22	m	m	[26] 20.22	m	m
28	MIME-Version	[26] 20.24	o	m	[26] 20.24	o	m
29	Min-Expires	[26] 20.23, [70] 5, 6	o	m	[26] 20.23, [70] 5, 6	o	m
30	Min-SE	[58] 5	o	o	[58] 5	m	m
31	Organization	[26] 20.25	o	o	[26] 20.25	o	o
32	P-Access-Network-Info	[52] 4.4	o	o	[52] 4.4	o	m
32a	P-Answer-State (Note3)	[34] 9.1	n/a	n/a	[34] 9.1	n/a	n/a
33	P-Asserted-Identity	[34] 9.1	n/a	n/a	[34] 9.1	o	m
33a	P-Asserted-Service	[121]	n/a	n/a	[121]	n/a	c1
33b	P-Associated-URI	[52] 4.1	n/a	n/a	[52] 4.1	c9	m
34	P-Called-Party-ID	[52] 4.2	n/a	n/a	[52] 4.2	n/a	c1
35	P-Charging-Function-Addresses	[52] 4.5	n/a	n/a	[52] 4.5	n/a	c1
36	P-Charging-Vector	[52] 4.6	n/a	n/a	[52] 4.6	n/a	c1
36b	P-Early-Media	[109] 8	o	m	[109] 8	o	m
38	P-Media-Authorization	[31] 6.1	o	o	[31] 6.1	o	o
39	P-Preferred-Identity	[34] 9.2	m	m	[34] 9.2	n/a	n/a
39a	P-Preferred-Service	[121] 4.2	n/a	n/a	[121] 4.2	n/a	c1
39b	P-Profile-Key	[97] 5	n/a	n/a	[97] 5	n/a	c1
39c	P-User-Database	[82] 4	n/a	n/a	[82] 4	n/a	c1
40	P-Visited-Network-ID	[52] 4.3	n/a	n/a	[52] 4.3	n/a	c1
40a	Path	[35] 4.2	o	o	[35] 4.2	m	m
41	Priority	[26] 20.26	n/a	n/a	[26] 20.26	n/a	c1

Item	Header	Sending (UE to P-CSCF)			Receiving (P-CSCF to UE)		
		Ref.	Profile status UNI (Gm)	Profile status UE	Ref.	Profile status UNI (Gm)	Profile status UE
41a	Priv-Answer-Mode	[158]	o	o	[158]	o	o
42	Privacy	[33] 4.2	o	m	[33] 4.2	m	m
43	Proxy-Authenticate	[26] 20.27	n/a	n/a	[26] 20.27	m	m
44	Proxy-Authorization	[26] 20.28	m	m	[26] 20.28	n/a	c1
45	Proxy-Require	[26] 20.29	n/a	n/a	[26] 20.29	n/a	c1
46	Rack	[27] 7.2	m	m	[27] 7.2	m	m
47	Reason	[34A] 2	o	n/a	[34A] 2	m	m
48	Record-Route	[26] 20.30	m	m	[26] 20.30	m	m
48A	Recv-Info	[25] 9.2.3	o	o	[25] 5.2.3	o	o
49	Referred-By	[59] 3	o	m	[59] 3	o	m
49b	Refer-Sub	[95]	n/a	n/a	[95]	n/a	C1
49c	Refer-to	[36] 3	c8	c8	[36] 3	c8	c8
50	Reject-Contact	[56B] 9.2	n/a	n/a	[56B] 9.2	n/a	c1
51	Replaces	[60] 6.1	o	o	[60] 6.1	o	o
52	Reply-To	[26] 20.31	o	o	[26] 20.31	o	m
53	Request-Disposition	[56B] 9.1	o	o	[56B] 9.1	o	o
54	Require	[26] 20.32	o	m	[26] 20.32	o	m
55	Retry-After	[26] 20.33	o	o	[26] 20.33	o	m
56	Route	[26] 20.34	m	m	[26] 20.34	n/a	n/a
57	RSeq	[27] 7.1	m	m	[27] 7.1	m	m
58	Security-Client	[48] 2.3.1	n/a	n/a	[48] 2.3.1	n/a	c1
59	Security-Verify	[48] 2.3.1	n/a	n/a	[48] 2.3.1	n/a	c1
60	Server	[26] 20.35	o	o	[26] 20.35	o	o
60b	Service-Route	[38] 5	n/a	n/a	[58] 4	o	m
61	Session-Expires	[58] 4	o	m	[58] 4	o	m
61b	Session-ID	See [Ref_dt1], Note 5	c5	c5	See [Ref_dt1], Note 5	c5	c5
62	SIP-Etag	[70] 11.3.1	o	n/a	[70] 11.3.1	o	o
63	SIP-If-Match	[70] 11.3.2	o	n/a	[70] 11.3.2	o	o

Item	Header	Sending (UE to P-CSCF)			Receiving (P-CSCF to UE)		
		Ref.	Profile status UNI (Gm)	Profile status UE	Ref.	Profile status UNI (Gm)	Profile status UE
64	Subject	[26] 20.36	o	o	[26] 20.36	o	m
65	Subscription-State	[28] 8.2.3	o	m	[28] 8.2.3	o	m
66	Supported	[26] 20.37	o	m	[26] 20.37	o	m
67	Timestamp	[26] 20.38	o	m	[26] 20.38	o	m
68	To	[26] 20.39	m	m	[26] 20.39	m	m
69	Unsupported	[26] 20.40	o	o	[26] 20.40	o	m
70	User-Agent	[26] 20.41	m	m	[26] 20.41	o	m
70a	User-to-User	[126]	o	o	[126]	o	o
71	Via	[26] 20.42	m	m	[26] 20.42	m	m
72	Warning	[26] 20.43	o	o	[26] 20.43	o	m
73	WWW-Authenticate	[26] 20.44	n/a	n/a	[26] 20.44	o	m

Conditions for Table 7-2:

c1: IF received discard or ignore Header.

c2: Applicable for authentication between UA

c3: This Header is only received within a SUBSCRIBE; see table A.5.

c4: IF CCBS THEN m ELSE o.

c5: IF 3PTY (INVITE) OR ECT (REFER) THEN m OR IF end to end correlation (all succeeding SIP messages following Initial Request within the Dialog) THEN o ;
Session ID must contain the hashed call id value.

c6: void.

c7: void.

c8: IF REFER THEN m ELSE n/a.

c9: If Registration THEN m.

NOTE 1: The use is only foreseen for the Deutsche Telekom domain.
NOTE 2: void.
NOTE 3: P-Answer-State header extension to the session initiation protocol for the open mobile alliance push to talk over cellular.
NOTE 4: Void.
NOTE 5: This Reference is shown within Section 2 of this document, because this is a requirement of Deutsche Telekom to align Calls all over the network.

7.3.5 MIME Types

The following MIME Types shall be supported:

Table 7.3.5.1: Supported MIME Types

Item	MIME Type	Sending (UE to P-CSCF)			Receiving (P-CSCF to UE)		
		Ref.	**Profile status UE**	**Profile status UNI (Gm)**	**Ref.**	**Profile status UE**	**Profile status UNI (Gm)**
1	application/vnd.etsi.pstn+xml	NOTE 1	c1	o	Note 1	c1	o
2	application/x-session-info	3GPP TS 29.163	o	o	3GPP TS 29.163	o	o
3	application/vnd.etsi.aoc+xml	3GPP TS 24.647	m	o	3GPP TS 24.647	m	o
4	application/simservs+xml	1TR126	m	o	1TR126	m	o
5	application/vnd.3gpp.cw+xml	3GPP TS 24.610	m	o	3GPP TS 24.610	m	o
6	application/sdp	RFC 2327	m	m	RFC 2327	m	m
7	application/pidf+xml	RFC 3863	o	o	RFC 3863	o	o
8	multipart/mixed		m	m		m	m
9	application/rlmi+xml		o	o		o	o
10	application/watcherinfo+xml	RFC 3858	n/a	n/a	RFC 3858	n/a	n/a
11	text/plain	RFC 2046	n/a	n/a	RFC 2046	n/a	n/a
12	image/t.38	RFC 3362	o	o	RFC 3362	o	o
13	application/simple-message-summary	RFC 3842	c2	o	RFC 3842	c2	o
14	other MIME types (NOTE 2)		n/a	n/a		n/a	n/a
15	encrypted MIME TYPE		n/a	n/a		n/a	n/a

NOTE: The references in this table are listed in the present document (see clause 2).

Conditions:

c1: IF ISDN is supported THEN m ELSE n/a.

c2: IF MWI is supported THEN m ELSE n/a.

NOTE 1: 3GPP the definition is within 3GPP TS 29.163.

NOTE 2: Other MIME Types can be received and must be discarded in case where no content disposition header is present or the MIME is not known.

7.3.6 SDP Types

See Annex B

7.4 SIP User Agent (UA)

NOTE: The references in the following tables are listed in the present document (see clause 2).

7.4.1 Supported SIP Signalling Transport Protocols in UA

The following SIP Signalling Transport Protocols shall be supported:

Protocol (NOTE)	Specification	Ref.	Support
UDP	RFC 0768/STD006	[34]	m
TCP	RFC 0793/STD007	[35]	m
TLS 1.2	RFC 5246	[88]	m
TLS 1.3	RFC8446	[201]	m
SCTP	ETSI TS 102 144	[5]	o
IPSec	RFC 2411	[44]	o
NOTE: The following combinations shall be possible to configure: ■ SIP over UDP ■ SIP over TCP without TLS ■ SIP over TCP with TLS NOTE: A change from UDP to TCP during a call setup is not allowed. If MTU size increases a UPD segmentation shall be done.			

Table 7.4.1.1: Supported SIP Signalling Transport Protocols in UA

7.4.2 Support of IPv4 und IPv6

Specification	Title	Ref.	Support
RFC 0791	Internet Protocol, Version 4	[35]	m
RFC 0792	Internet Control Message Protocol	[36]	m
RFC 1035	Domain names implementation and specification	[38]	m
RFC 2460	Internet Protocol, Version 6	[40]	m
RFC 2782	A DNS RR for specifying the location of services (DNS SRV)	[47]	m
RFC 2915	The Naming Authority Pointer (NAPTR) DNS Resource Record	[48]	o
RFC 3596	DNS Extensions to Support IP Version 6	[54]	m
RFC 4443	Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification; March 2006	[64]	m
RFC 4884	Extended ICMP to Support Multi-Part Messages, April 2007	[70]	m

Table 7.4.2.1: Support of IPv4 und IPv6

Procedure	Specification	Ref.	Support
DNS SRV-record	RFC 3263	[50]	m
DNS NAPTR-record	RFC 3263	[50]	o

Table 7.4.2.2: DNS Records

Protocol	Remarks	Support
Static Routing	Preconfigured SIP server IP address in UA.	m
DNS A-record	Preconfigured SIP server fully qualified domain name in UA.	m
DNS AAAA-record	Preconfigured SIP server fully qualified domain name in UA.	m

Table 7.4.2.3: Procedures for SIP-Server Localisation

7.4.3 Video Codec Transport Procedures

Specification	Title	Ref.	Support
RFC 2190	RTP Payload Format for H.263 Video Streams	[41]	m
RFC 2429	RTP Payload Format for the 1998 Version of ITU-T Rec. H.263 Video (H.263+)	[45]	m
RFC 3984	RTP Payload Format for H.264 Video	[60]	o
RFC 2032	RTP Payload Format for H.261 Video Streams	[39]	o

Table 7.4.3.1: Specifications Video Codec Transport Procedures

7.4.4. Real-time Transport Procedures

Specification	Title	Ref.	Support
RFC 3550	RTP: A Transport Protocol for Real-Time Applications; July 2003	[53]	m
RFC 4040	RTP Payload Format for a 64 kbit/s Transparent Call; April 2005 (see NOTE)	[62]	c1
RFC 3711	The Secure Real-time Transport Protocol (SRTP)	[76]	m NOTE 3 NOTE 5
RFC 4568	Session Description Protocol (SDP) Security Descriptions for Media Streams	[77]	m NOTE 3 NOTE 4
RFC4961	Symmetric RTP / RTP Control Protocol (RTCP)	[93]	m
RFC 4347	Datagram Transport Layer Security	[78]	o

Conditions (Notes are mandatory to be supported):

c1: If ISDN interworking then m else o.

NOTE 1: This protocol is applicable to carry 64 kbit/s channel data transparently in RTP packets, using a pseudo-codec called "Clearmode" and is used in case of ISDN accesses via IADs, only.

NOTE 2: Fragmented IP packets are not supported by the IMS platform of Deutsche Telekom. If the UA chooses to send RTCP/SDES packets it shall not send the UA's public IP address.

NOTE 3: More detail is given in 1 TR 114 ANNEX B Section 4.2B.2 Media security. When media security is needed the Secure Real-time Transport Protocol (SRTP) according to RFC 3711 [76] shall be used

NOTE 4: Encryption Algorithm AES (Advanced Encryption Standards), IP transport UDP and Authentication method SHA-1 cryptographic hash function shall be supported.

NOTE 5: The following requirements has to be fulfilled: Exchange of Master Keys over SDES (Security Descriptions for Media, SDES (Security Descriptions for Media Streams) in SIP/SDP, building of Session Keys from Master Key and Encryption Key (encryption of Payloads)

NOTE 6: "Security Mechanism Names for Media" draft-dawes-dispatch-mediasec-parameter-07.txt [79] shall be considered in addition.

NOTE 7: As a hint for implementation: RFC3605 is not supported. An implementation of RFC 3605 in UE's may lead to unsuccessful calls.

Table 7.4.4.1: Specifications Real-time Transport Procedures

8 SIP terminals

SIP terminals can be connected to the NGN platform of Deutsche Telekom in two ways:

- By connecting directly to the Internet, e.g. via a Network Access Server (NAS)
- As part of a local network whose local router (NAT Router) is connected to the Internet by means of a Network Access Server

SIP terminals can use IPv4 or IPv6 to communicate with the call control. The communication (Signalling and Media) of an UA shall be based either on IPv4 or IPv6. If both protocols available, IPv6 shall be preferred.

8.1 Direct connection

The SIP Client is either a hard phone (physical IP telephone) or a soft phone (software client). This type of connection is characterized by the fact that the SIP Client can be reached via the IP address assigned by the NAS or via a fixed IP address.

8.2 Local network

One or more SIP terminals can also be part of a local network. In this environment, every SIP Client has its own private IPv4 address in the local network. Starting from the NGN platform of Deutsche Telekom, both SIP Clients are talked to with the same external address. However, the NGN platform of Deutsche Telekom uses different ports here for the individual clients here. A local router is responsible for converting the external IPv4 address to the internal IPv4 address and transport protocol port number. This conversion is known as Network Address (Port) Translation (NAPT). The rules for NAPT shall be stored in the local router.

Where necessary, a SIP Client enters its internal IP address in the SIP messages. Taking the rules described above, the NGN platform of Deutsche Telekom translates the internal IP addresses to the external IP addresses.

In order to eliminate the necessity of IPv6 packet fragmentation for IPv4 packets that have to be translated by the Call Control into IPv6 packets, a SIP client shall not send RTP messages with maximum transmission units (MTU) larger than 1260 bytes. When choosing 1260 bytes as MTU for IPv4 packets the IPv4 to IPv6 translation within the Call Control will lead to in maximum 1280 bytes large IPv6 packets - a MTU size that can be handled by all IPv6 capable link types without IPv6 packet fragmentation.

Over and above that an adoption of the IPv4 MTU of 576 bytes for IPv4 and IPv6 RTP packets is strongly recommended for all SIP clients. In order to minimize delay, jitter and packet loss the fragmentation of IP packets shall be avoided. In the IPv4 header of an RTP packet the value of the DF bit in the Flag field shall be "1" (Don't Fragment).

When receiving an ICMPv4 'Destination Unreachable' message with error code '4' (fragmentation needed and DF set) the SIP client shall use the 'Next-Hop MTU' info (RFC4884) [70] of this ICMP error packet to limit its MTU to the given value."

When the SIP terminal uses IPv6, the IPv6 address is a global address. NAPT shall not be used.

"When using IPv6 the SIP client shall limit its IPv6 MTU size for RTP packets to 1280 bytes. Nevertheless a MTU size of 576 bytes is also recommended for IPv6 based RTP packets."

The local router can be one of the following devices, for example:

- DSL router
- WLAN router

8.3 Support of IPv6 by the UE

The set of IPv6 functionality a 3GPP UE will require is dependent on the services (IMS, Packet Streaming etc.) it will use. As a minimum, a 3GPP UE shall comply with the Basic IP group of specifications as defined in RFC 3316 [51] (chapter 2). This IPv6 functionality is sufficient to provide compatibility towards IPv6 entities external to 3GPP. To ensure network performance the UE shall limit the sending packet size of media data to 1280 octets; to ensure this and the requirements of RFC 3316, the UE has to support RFC 4443 [64] (chapter 3). Nevertheless a MTU size of 576 bytes is also recommended for IPv6 based RTP packets."

According to the procedures defined in TS 23.060 [18] and in TS 23.401 [20], when a UE is assigned an IPv6 prefix, it can change the global IPv6 address it is currently using via the mechanism defined in RFC 3041, or similar means, without updating the PS domain. Any application that requires full IP address knowledge shall provide a mechanism to get the latest IPv6 address when the IPv6 address in the UE has been changed.

An example of such means is defined in TS 23.228 [19].

NOTE: RFC 3316 [51] does not make any recommendations on preferred transition and interoperability mechanisms between IPv4 and IPv6.

8.4 Network Access

Description of minimum technical requirements for potential QoS transport (up-/downstream).

8.4.1 General User Equipment (UE) requirements

The packetization size has to be equal or more than 20ms to ensure two high quality media streams using the codec G.711a or G.722 over the guaranteed bandwidth on the SIP (Gm) interface of Deutsche Telekom.

Due to this requirement, the UE shall support the following features:

- The packetization size shall be increased to 30ms if necessary.
- The switching between 10ms, 20ms or 30ms packetization size might happen automatically according to the available bitrate.

8.4.2 Traffic Classes in Layer 3

The UE uses the following traffic classes at Layer 3 (according to the Architecture of Deutsche Telekom)

- Voice Control Class 6 (DSCP 110 000)
- Voice Bearer Class 5 (DSCP 101 110)
- PPP/PPPoE Control Traffic Class 6
- Best Effort Class 0 (DSCP 000 000)

Prioritisation & marking should always be processed internally at the UE, even when the network connection does not support VLAN tags for prioritisation.

The traffic classes used shall be the same, independently whether IPv4 or IPv6 is used.

Authorized traffic & signalling should be marked, tagged and prioritized at the UE towards to the Deutsche Telekom platform. All other traffic should be marked and scheduled as Best Effort (assumption is that LAN bandwidth is larger than towards Deutsche Telekom platform).

8.4.3 Service Creation

Note that this chapter gives only a functional description of possible interaction with the platform. The QoS agreement respectively the service creation depends on the Service Level Agreement. Deutsche Telekom gives no service guarantee neither for the received traffic class or for the transparent transport of code points nor for VLANs or other protocol types.

8.5 Number handling by the UE

Generally, concerning UEs there are no requirements for any kind of number handling.

The UE shall not alter the dialled number by the user when sending to the NGN platform of Deutsche Telekom.

All phone numbers beginning with “11” (short codes, e.g. 112 or 110 or 11833; see also national number plan of Germany) shall not be manipulated by any UE; these numbers shall be sent out without any Country Code (CC) or National Destination Code (NDC).

NOTE: Each connection to a 11xyz destination including a CC and/or a NDC has to be rejected in the NGN platform of Deutsche Telekom according to regulation requirements.

8.6 Support of NAT traversal by the UE

In general endorsement of 3GPP TS 24.229 [21] Annex F and Annex K is valid with the following extensions.

For keeping the NAT-Pinholes open, and depending on the transport protocol for SIP signaling, the following packet type shall be sent by the UE to the next hop SIP port:

- Basic keepalive,
- Empty UDP messages,
- TCP single CRLF.

For keeping the NAT-Pinholes open for media, one of the following packet types shall be sent by the UE to the next hop session media ports.:

- Empty RTP packets, as follows

  To keep NAT bindings and firewall pinholes open with uni-directional RTP traffic and enable the C-BGF to perform address latching, the UE shall send keep alive messages for each media stream. These messages shall be sent regardless of whether the media stream is currently inactive, send only, recvonly or sendrecv. It is recommended that the keepalive message be an empty (no payload) RTP packet with a payload type of 20 as long as the other end has not negotiated the use of this value. If this value has already been negotiated, then some other unused static payload type from Table 5 of RFC 3551 [89] shall be used.

- RTCP packets

  Per session, keepalive packets shall be sent for each media stream and media stream component, i.e. RTP and RTCP

Re-Register messages shall not be used for maintaining NAT Pinholes.

8.7 UE receiving RTP from un-trusted sources

The UE device shall only process RTP & RTCP, received on its WAN interface, from A-BGF (Access Border Gateway Function) source IPs (IPv4 or IPv6) and Ports which were negotiated within the related SIP Session. RTP & RTCP Packets received from other sources shall be ignored and dropped.

NOTE: Depending on the network architecture an INVITE received may indicate different IP address for the sender of the SIP signalling and for the sender of the RTP & RTCP packets received.

8.8 Message Size

A SIP Message Size of 8kB shall be supported to guarantee a successful call setup.

NOTE: One example for such large calls is a VoLTE emergency call with UE provided location information.

9 Interworking requirements for SIP user equipment (UE)

The interworking requirements for SIP user equipment (e.g. IAD) are specified in separate documents. The referenced documents can be interpreted as recommendations for SIP terminal developers and vendors.

9.1 Analogue (POTS) – SIP basic interworking requirements

The Analogue / (POTS) – SIP basic interworking requirements are contained in the technical specification 1 TR 126.

9.2 DSS1 – SIP basic interworking requirements

The DSS1 – SIP basic interworking requirements are contained in the technical specification 1 TR 127 [4].

10 Procedures for TCP Non-Reachability

10.1 Setup of TCP session

The TCP session shall only be set up when required by the application layer, i.e., an upcoming SIP REGISTER shall trigger a TCP session set up.

The TCP session shall only be set up to the primary location received in the DNS reply.

The TCP session shall be set up sequentially to the three locations received in the DNS reply.

10.2 TCP-SYN Retry

In case the target does not reply, a maximum of 3 retries with doubled waiting time shall be done, i.e.

1. retry after 3 sec
2. retry after 6 sec
3. retry after 12 sec

If the target does not reply after the third retry, no further retries shall be executed.

This also applies to TCP connection set ups to secondary and tertiary locations.

10.3 Switch to failover location

In case of non-reachability, the switch to the failover location shall occur application driven.

If the application has not received an answer of the primary location to the REGISTER Request after 32 sec, the application shall send a new REGISTER to the secondary location received per eDNS.

Only then, based on application layer needs, a TCP connection shall be set up to the secondary location.

Similar applies if the secondary location is not reachable and a switch to the tertiary location is required.

10.4 All three targets are not reachable

If all three targets are not reachable, the flow recovery procedures according to IETF RFC 5626 [68] shall apply, i.e. the retry timer will be randomized per end device in a certain time frame. If the retry value is e.g. set to 600 sec, every end device is assigned a random value between 300 and 600 sec. The time frame is between 32 and 1800 sec.

The flow recovery procedure according to IETF RFC 5626 [68] affects the application layer and is hence only used in conjunction with the above-described TCP behaviour.

10.5 SIP 503 Retry after Handling

In case a SIP 503 with Retry After is received, the end device shall act as follows:

- Application layer: The end device shall remain on site
- TCP layer: The end device shall terminate the existing TCP session and re-create it with the new REGISTER after the Retry-After timer has ended.

In case a SIP 503 without Retry After is received, the end device shall act as follows:

- Application layer: The end device shall switch to the secondary location received per DNS reply
- TCP layer: The procedures for a switch to the failover location as per clause 10.3 shall apply.

Annex A Void

Annex B 3GPP TS 24.229 V11.6.0 (2012-12): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (Release 11) Modified version for SIP (Gm) interfaces provided by Deutsche Telekom only !

The protocol specification of the SIP (Gm) interface for SIP UE intended to be connected to xDSL accesses of Deutsche Telekom are described in the specifically modified 3GPP Standard TS 24.229 11.6.0 (2129-12).

The modifications in this 3GPP standard assure the compatibility with the NGN platform of Deutsche Telekom.

The modified specification is available as a PDF file with the following file name:

- 1TR114 Annex B_V020000_TS24229-b60.pdf

NOTE: The modified text that is added or deleted is shown as cursive and underlined (*example for added text*) or cursive and stricken (*~~example for stricken text~~*).

Annex C Service functionality requirements

This annex C describes the service functionality requirements as a recommendation for the behaviour of SIP user equipment connected to the NGN platform of Deutsche Telekom.

The following services are based on referenced ETSI or 3GPP standards. Deviations to these standards are explicitly defined in the present document. These services are defined as "Simulation Services" for the NGN platform of Deutsche Telekom.

Only the relevant clauses with the used options of these standards are provided in this section.

The actual numbering of the referenced documents are kept in the following with a leading "§" sign. Further on the references given in these clauses refer to the according document.

NOTE: For SIP trunk according to 1TR118 [91]/1TR119 [92] the service implementation may differentiate. More information is given in 1TR118 [91]

Annex C.1 Global definitions

For all services the "Ut" interface (XML) is currently not used by the NGN platform of Deutsche Telekom.

A later implementation is not generally excluded.

NOTE 1: The relevant service code commands (SCC) for provision/withdrawal, registration/erasure, activation/de-activation, interrogation and invocation are provided in Annex D.

NOTE 2: The activation/de-activation/ registration/erasure and interrogation of most of the following services are also possible via other methods (e.g. Web interface).

Annex C.2 Simulation services

The network centric feature logic for HOLD, CW, TOGGEL and CONF are currently available; therefore these features may be implemented locally on the SIP Client.

C.2.1 CDIV (Communication Diversion)

The relevant standard for the CDIV services is 3GPP TS 24.604. The determinations of options and deviations to this standard are defined in the following sections.

NOTE: For SIP trunk according to 1TR118 [91]/1TR119 [92] the service implementation may differentiate. More information is given in 1TR118 [91]

C.2.1.1 Currently supported CDIV services

Various methods of communication diversion are implemented in the NGN platform of Deutsche Telekom.

The following CDIV services are currently supported by Deutsche Telekom:

- CFU (Communication Forwarding Unconditional)1,
- CFB (Communication Forwarding Busy),
- CFNR (Communication Forwarding No Reply),

[1] While CFU services are activated the special dial tone shall be played in off-hook state (e.g. after picking up the receiver) instead of normal dial tone to remember the user that no incoming calls will be received.

- CFNL (Communication Forwarding on Not Logged-in),
- CFNRc (Communication Forwarding on Subscriber Not Reachable) [1]

C.2.1.2 Currently not supported CDIV services

The following CDIV services are currently not supported in the NGN platform of Deutsche Telekom:

- CDIVN (Communication Diversion Notification)

C.2.2 CONF (Conference)

The relevant standard for the CONF service is 3GPP TS 24.605.

NOTE: Concerning clause §4.5.2.1 "Actions at the originating UE", the relevant 3PTY procedures described in 1TR126 Annex B [3] shall apply in addition.

C.2.3 MWI (Message Waiting Indication)

Deutsche Telekom network does not support MWI. If MWI is implemented as an Option it shall be deactivated per default.

C.2.4 OIP/OIR (Originating Identification Presentation and Originating Identification Restriction)

The relevant standard for the OIP/OIR service is 3GPP TS 24.607. The determinations of options and deviations to this standard are defined in the following sections.

NOTE: For SIP trunk according to 1TR118 [91] / 1TR119 [92] the service implementation may differentiate. More information is given in 1TR118 [91]

§4.5.2.1 Actions at the originating UE

As part of basic communication, the originating UE may insert a P-Preferred-Identity header field in any initial SIP request for a dialog or in any SIP request for a standalone transaction as a hint for creation of a public user identity as described in 3GPP TS 24.229 [3].

NOTE 1: According 3GPP TS 24.229 [3], the UE can include any of the following in the P-Preferred-Identity header field:

a public user identity which has been registered by the user;

a public user identity returned in a registration-state event package of a NOTIFY request as a result of an implicit registration that was not subsequently deregistered or has expired; or

any other public user identity which the user has assumed by mechanisms outside the scope of 3GPP TS 24.229 [3] to have a current registration.

If the originating user wishes to override the default setting of "presentation not restricted" of the OIR service in temporary mode:

- ~~*The originating UE shall include an "anonymous" From header field. The convention for configuring an anonymous From header field described in IETF RFC 3323 [6] should be followed; i.e. From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag= xxxxxxx.*~~

[1] Communication Forwarding on Subscriber Not Reachable shall be seen as "Anrufweiterschaltung sofort im Störungsfall" (CDIV:CFU Stö). In this case the communication is forwarded to an announcement.

For the NGN platform of Deutsche Telekom the sending of From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=xxxxxxx is not allowed.

- If only the P-Asserted-Identity needs to be restricted the originating UE shall include a Privacy header field [6] set to "id" in accordance with IETF RFC 3325 [7].

  This Option is not used for OIR within the NGN platform of Deutsche Telekom. At least the privacy header must be identified by the AS and will be completed with the other privacy values "user" and "header".

- If all headers containing private, that the UE cannot anonymize itself, information need to be restricted the originating UE shall include a Privacy header field set to "header" in accordance with IETF RFC 3323 [6].

NOTE 2: The From header field is not anonymized by the Privacy header field value "header".

NOTE 3: In each case the From header shall contain a PUID.

*The following section is only valid for **CLIR 1** Service (See Section D.2):*

If the originating user wishes to override the default setting of "presentation restricted" of the OIR service in temporary mode:

- The originating UE shall include a Privacy header field of privacy type "none" in accordance with 3GPP TS 24.229 [3] (IETF RFC 3323 [6]) *and CLIR 1*.

*In normal presentation cases (**CLIP permanent**) the setting of "none is "forbidden.*

If the display name is used then it shall have the same content as the accompanying uri. The device MUST NOT allow a user defined "display name".

§4.5.2.12 Actions at the terminating UE

Add following text:

The identity presented to the user shall be the From header field. In addition, the P-Asserted-Identity may be presented.

C.2.5 TIP/TIR (Terminating Identification Presentation and Terminating Identification Restriction)

The relevant standard for the TIP/TIR service is 3GPP TS 24.608. The determinations of options and deviations to this standard are defined in the following sections.

Note: For SIP trunk according to 1TR118 [91]/1TR119 [92] the service implementation may differentiate. More information is given in 1TR118 [91]

Add text to 4.5.2.1 Actions at the originating UE

If the originating user is subscribed to the TIP services and wants to receive changes of the terminating identity in the dialog, the UE shall add the option tag "from-change" to the Supported header field in the initial request.

C.2.6 HOLD (Communication HOLD)

NOTE: For SIP trunk according to 1TR118 [91]/1TR119 [92] the service implementation may differentiate. More information is given in 1TR118 [91]/1TR119 [92]

The relevant standard for the HOLD service is 3GPP TS 24.610.

The actions in Section "4.5.2.1 Actions at the invoking UE" shall apply with the following general modification:

- Only re-INVITE shall be used.

- The bandwidth indicated by the bandwidth attribute according to RFC 3890 [58] shall be used.

NOTE: 0.0.0.0 shall not be used for HOLD procedures.

C.2.7 ACR and CB (Anonymous Communication Rejection and Communication Barring)

The relevant standard for the ACR and CB service is 3GPP TS 24.611 [9].

C.2.8 CW (Communication Waiting)

Based on the VGW (IAD) configuration and it must be possible to activate a local/terminal based CW on a busy line if an INVITE without a CW indication is received by the VGW. The default for local/terminal based CW is deactivated.

The relevant standard for the CW service is 3GPP TS 24.615 [22].

The sections "4.5.5.1 Actions at the UE of user C" and "4.5.5.3 Actions at the UE of user B" in 3GPP TS 24.615 [22] shall apply.

To avoid loss in QoS, a maximum of 2 active and 2 waiting communications shall apply.

NOTE: To avoid "ghost ringing", a UE while in idle state should not signal an incoming communication (by any acoustical or visual signal, e.g. ringing signal or display information) based on a SIP request INVITE with XML: call-waiting-indication.

C.2.9 MCID (Malicious Communication Identification)

The relevant standard for the MCID service is 3GPP TS 24.616. The determinations of options and deviations to this standard are defined in the following sections:

§4.5.2.12.1 Subscriber has a temporary subscription

In case of invoking the MCID service the UE shall sent a ~~*Re-INVITE*~~ *initial INVITE including a Service Code Command*.

NOTE: The Service Code Commands for invocation are defined in Annex D.
~~*As a network operator option including a XML-MIME with XML mcid body with MCID XML Request schema containing a McidRequestIndicator set to 1 could be sent.*~~

C.2.10 ECT (Explicit Communication Transfer)

The relevant standard for the ECT service is 3GPP TS 24.629. The determinations of options and deviations to this standard are defined in the following sections.

§4.4 Coding requirements

A user agent that wishes to use the ECT service (to act as a transferor):

- Shall support the REFER method as a client as specified in RFC 3515 [2].
- Shall support the Referred-By header as specified in RFC 3892 [3].

A user agent that is the transferred party in a communication transfer (acts as the transferee):

- ~~*Shall support the REFER method as a server as specified in RFC 3515 [2].*~~
- ~~*Shall*~~ *May* support the Referred-By header as specified in RFC 3892 [3].

- ~~Shall~~ May support Replaces header field as a client as specified in RFC 3891 [4].

A user agent that is the transfer target in a communication transfer:

- May support the Referred-By header as a server as specified in RFC 3892 [3].
- May support the Replaces header as a server as specified in RFC 3891 [4].

§4.5.2.1 Actions at the transferor UE

A UE that initiates a transfer operation shall:

- Issue a REFER request in the original communications dialog, where:
  - The request URI shall contain the SIP URI of the transferee as received in the Contact header field.
  - The Refer-To header field shall indicate the public address of the transfer Target.
  - *~~If the transferor UE has a consultation communication with the transfer Target, a~~* A Replaces header field parameter shall be added to the Refer-To URI together with a Require=replaces header field parameter.

    NOTE: The NGN platform of Deutsche Telekom supports only consultative ECT for confirmed communications.
  - The Referred-By header field may indicate the identity of the transferor.
  - *The REFER shall contain a Session-ID header field.*

After the REFER request is accepted by the other end with a 202 (Accepted) response, the transferor UE should get notifications of how the transferee's communication setup towards the transfer Target is progressing.

When a NOTIFY request is received on the REFER dialog that indicates that the transferee and the transfer Target have successfully setup a communication, the transferor UE *shall*~~may~~ terminate the original communication with the transferee UE, by sending a BYE message on the original dialog.

§4.5.2.5 Actions at the transferee UE

Basic communication procedures according to 3GPP TS 24.229 [2] shall apply.
~~When a REFER request is received in the context of a call transfer scenario (see clause 4.5.2.4.1), the transferee UE shall perform the following steps:~~

~~1) apply the procedure for holding the active communication with the transferor as described in TS 183 010 [8] clause 4.5.2.1; and~~

~~2) apply normal REFER handling procedures according to ES 283 003 [1].~~

§A.2 Consultative transfer

NOTE: The HOLD call flow as described in Annex A, A.2 shall not apply; the call flow as defined in Annex B of 1TR126 [3] shall apply accordingly.

C.2.11 CCBS/CCNR/CCNL (Completion of Communications to Busy Subscriber/ Completion of Communications by No Reply/ Completion of Communication on Not Logged-in)

The relevant standard for the CCBS service is 3GPP TS 24.642 [23]. The determinations of options and deviations to this standard are defined in the following sections.

C.2.11.1 Global modification

The NGN platform of Deutsche Telekom sends a 199 for the release of early dialogs. A further 18x response (e.g. 180 in case of CCNR activation rejection) may be sent afterwards.

§4.5.4.1 Actions at the originating UE

Basic call procedures ~~*and in case of a call-completion recall initiated by a REFER request, normal REFER method handling procedures*~~ according to 3GPP TS 24.229 [2] shall apply.

For invoking and revoking of the call completion services, announcement procedures according to 3GPP TS 24.628 [3] and inband-interaction procedures *shall*~~*should*~~ be used.

C.2.12 AOC (Advice Of Charge)

NOTE: For SIP trunk according to 1TR118[91]/1TR119 [92] the service implementation may differentiate. More information is given in 1TR118[91]/1TR119 [92]

The relevant standard for the AOC service is 3GPP TS 24.647 [10].

Advice of charge (AOC) information shall be treated according 3GPP TS 24.647 [10], Annex D „AOC XML Schema“.

During a communication different AOC types (e.g. AOC-D) can be used to convey tariff and/or cost information. All types of AOC described in 3GPP TS 24.647 [10] are supported, depending on the requested service options on the subscriber line.

AOC tariff information will only be conveyed in monetary format (currency), but not in non-monetary format (units).

If two communications have been established via the UE (e.g. in case of HOLD, Toggle or 3PTY), the UE receives separate AOC XML’s for each communication.

C.2.12.1 AOC-S

The AOC-S service provides tariff information at the beginning of a communication and when tariff changes occur during a communication.

AOC-S information can be conveyed in the following SIP messages:

- reliable 18x message
- 200OK (INVITE)
- INFO

The AOC-S tariff-information can be expressed as:

- Monetary price per time unit and time unit (basic-type->price-time);
- Monetary flat rate (communication-setup->flat-rate).

C.2.12.2 AOC-D

The AOC-D service provides tariff information about the recorded charges during the active phase of a communication.

Only accumulated charges in monetary format are transmitted.

AOC-D information can be conveyed in the following SIP messages:

- INFO
- BYE
- Final response (BYE)

C.2.12.3 AOC-E

The AOC-E service provides tariff information about the recorded charges for a communication when it is terminated.

Only accumulated charges in monetary format are transmitted.

AOC-E information can be conveyed in the following SIP messages:

- BYE
- Final response (BYE)

Annex D Service code commands (SCC) and Service Order Commands (SOC)

Annex D gives an overview of the supplementary services provided by the NGN platform of Deutsche Telekom and the corresponding Service Code Commands (SCC) as well as the Service Order Commands (SOC). These SCC/SOC allow the control of service features by the subscriber via the UE.

Which services actually are provided by the NGN platform of Deutsche Telekom must be taken from the AGB [1] of Deutsche Telekom.

The implementation of this Annex is not relevant for implementations according to 1TR118 [91]/1TR119 [92]

NOTE: Further on, the instruction manual of a particular service has to taken into account.

A Service Code Commands can be made up by "*" (star), "#" (hash) and/or figures; a Service Order Commands can be made up by a Hook Flash function and a figure (usually one digit).

Depending on the service, a SCC can be used to activate, deactivate, interrogate or invoke a specific service feature. For some of these services a PIN is needed for service modifications.

NOTE: The "Hook Flash" function initiated by the user on a UE has to be mapped to SIP messages in the relevant SIP client, accordingly.

Syntax:

The following syntax rules are used for the SCC/SOC:

< > Information in pointed brackets is an obliged input (signs or figures)

NOTE: See also clause 3.1 Symbols.

Annex D.0 Overview of the supplementary services

The following table gives an overview of the currently supported supplementary services in the NGN platform of Deutsche Telekom.

Clause	Service / Supplementary service	Abbr.
D.1	Calling Line Identification Presentation / Originating Identification Presentation [Anzeige der Rufnummer des Anrufers]	CLIP/OIP
D.2	Calling Line Identification Restriction / Originating Identification Restriction [Unterdrückung der Rufnummernanzeige des Anrufers]	CLIR/OIR
D.3	Connected Line Presentation / Terminating Identification Presentation [Anzeige der Rufnummer des Angerufenen]	COLP/TIP
D.4	Connected Line Restriction/Terminating Identification Restriction [Unterdrückung der Rufnummernanzeige des Angerufenen]	COLR/TIR
D.5	Call Waiting / Communication Waiting [Anklopfen]	CW
D.6	Hold / Toggle [Rückfrage/Makeln]	HOLD/TOGGLE
D.7	Three Party Conference / Conference [Dreierkonferenz]	3PTY/CONF
D.8	Call Forwarding Unconditional / Communication Forwarding Unconditional [Anrufweiterschaltung sofort]	CDIV:CFU
D.9	Call Forwarding Busy / Communication Forwarding Busy [Anrufweiterschaltung bei Besetzt]	CDIV:CFB
D.10	Call Forwarding No Reply / Communication Forwarding No Reply [Anrufweiterschaltung bei Nichtmelden]	CDIV:CFNR
D.11	Selective Call Forwarding Unconditional / Selective Communication Forwarding Unconditional [Anrufweiterschaltung selektiv sofort]	CDIV:S-CFU
D.12	Selective Call Forwarding Busy/Selective Communication Forwarding Busy [Anrufweiterschaltung selektiv bei Besetzt]	CDIV:S-CFB
D.13	Selective Call Forwarding No Reply / Selective Communication Forwarding No Reply [Anrufweiterschaltung selektiv bei Nichtmelden]	CDIV:S-CFNR
D.14	Selective Call Forwarding / Selective Communication Forwarding – Deletion/Reset [Anrufweiterschaltung selektiv - aufheben/löschen]	-
D.15	Communication Forwarding on Not Logged-in [Anrufweiterschaltung bei offline/nicht registriert]	CFNL
D.16	Communication Barring - Incoming Communication Barring [Sperren kommend – Alle eingehenden Anrufe abweisen]	ICB
D.17	Communication Barring - Forwarded Communication Barring [Sperren kommend – Alle weitergeleiteter Verbindungen abweisen]	-
D.18	Communication Barring - Anonymous Communication Rejection [Sperren kommend – Alle unbekannten Anrufer abweisen]	ACR

D.19	Communication Barring – Incoming Communication Barring: White list [Sperren kommend – Nur Anrufer aus Positivliste zulassen]	-
D.20	Communication Barring – Incoming Communication Barring: Black list [Sperren kommend – Alle Anrufer aus Negativliste abweisen]	-
D.21	Communication Barring –Incoming Communication Barring: Virtual Black list / Kick Out [Sperren kommend – virtuelle Negativliste (Blacklist – Kick Out)]	-
D.22	Communication Barring - Outgoing Communication Barring [Sperren gehend – alle und selektiv (Wahlsperren)]	OCB
D.23	Communication Barring –Outgoing Communication Barring: White list [Sperren gehend – Nur Anrufe auf Positivliste zulassen (Whitelist)]	-
D.24	Communication Barring – Outgoing Communication Barring: Black list [Sperren gehend – Alle Anrufe auf Negativliste abweisen (Blacklist)]	-
D.25	Completion of Call to Busy Subscriber /Completion of Communications to Busy Subscriber [Rückruf bei Besetzt]	CCBS
D.26	Completion of Call on No Reply/Completion of Communications by No Reply [Rückruf bei Nichtmelden]	CCNR
D.27	Completion of Call on Not Logged-in [Rückruf bei Nichtregistriert]	CCNL
D.28	Explicit Call Transfer/Explicit Communication Transfer [Zusammenschalten von Verbindungen]	ECT
D.29	PIN modification [PIN Modifizierung]	-
D.30	Reset [Zurücksetzen von LM auf Defaultwerte]	-
D.31	Malicious Call Identification/Malicious Communication Identification [Identifizieren/Fangen]	MCID

Table Annex D0-1: Overview of the supplementary services

NOTE 1: For some services no abbreviations are still defined.

NOTE 2: Some official abbreviations are modified for certain services used within the NGN platform of Deutsche Telekom.

Annex D.1 Calling Line Identification Presentation /Originating Identification Presentation (CLIP/OIP)

D.1.1 Procedures

D.1.1.1 Activation

(wait for dial tone) *30*<PIN># (wait for ack.)

D.1.1.2 Deactivation

(wait for dial tone) #30*<PIN># (wait for ack.)

D.1.1.3 Interrogation

(wait for dial tone) *#30# (wait for ack.)

Annex D.2 Calling Line Identification Restriction /Originating Identification Restriction (CLIR/OIR)

D.2.0 Description

CLIR 1: While calling line identification restriction is set to permanent mode, the subscriber can deactivate the calling line identification restriction on per communication basis. If this service is deactivated for an outgoing communication, the calling line identification is presented to the called party for this communication; after this communication the permanent CLIR is automatically activated, again.

CLIR 2: While calling line identification presentation is set to permanent mode, the subscriber can activate the calling line identification restriction on per communication basis. If this service is activated for an outgoing communication, the calling line identification is restricted for this communication; after this communication the CLIR is automatically deactivated, again.

CLIR 3: Permanent calling line identification restriction: This service do NOT allow the subscriber to activate or deactivate the CLIR service permanently.

CLIR: Permanent calling line identification restriction: This service allows the subscriber to activate or deactivate the CLIR service permanently. The selected CLIR mode may be temporarily changed by using CLIR1 or CLIR2.

NOTE: Control of all CLIR supplementary services is only possible if the specific feature CLIR 3 (permanent CLIR for all lines) is not activated/booked.

D.2.1 Procedures

D.2.1.1 Activation

D.2.1.1.1 CLIR1/OIR1

(wait for dial tone) #31#<DN>

D.2.1.1.2 CLIR2/OIR2

(wait for dial tone) *31#<DN>

D.2.1.1.3 CLIR/OIR

(wait for dial tone) *32*<PIN># (wait for ack.)

D.2.1.2. Deactivation

D.2.1.2.1 CLIR1/OIR1

(automatically)

D.2.1.2.2 CLIR2/OIR2

(automatically)

D.2.1.2.3 CLIR/OIR

(wait for dial tone) #32*<PIN># (wait for ack.)

D.2.1.3 Interrogation

D.2.1.3.1 CLIR1/OIR1

Not applicable.

D.2.1.3.2 CLIR2/OIR2

Not applicable.

D.2.1.3.3 CLIR/OIR

(wait for dial tone) *#32# (wait for ack.)

Annex D.3 Connected Line Identification Presentation / Terminating Indication Presentation (COLP/TIP)

D.3.1 Procedures

D.3.1.1 Activation

(wait for dial tone) *40*<PIN># (wait for ack.)

(wait for dial tone) *40*<PIN>*0# (wait for ack.) (for all VoIP lines)

D.3.1.2 Deactivation

(wait for dial tone) #40*<PIN># (wait for ack.)

D.3.1.3 Interrogation

(wait for dial tone) *#40# (wait for ack.)

Annex D.4 Connected Line Identification Restriction / Terminating Indication Restriction (COLR/TIR)

D.4.1 Procedures

D.4.1.1 Activation

(wait for dial tone) *42*<PIN># (wait for ack.)

(wait for dial tone) *42*<PIN>*0# (wait for ack.) (for all VoIP lines)

D.4.1.2. Deactivation

(wait for dial tone) #42*<PIN># (wait for ack.)

D.4.1.3 Interrogation

(wait for dial tone) *#42# (wait for ack.)

Annex D.5 Call Waiting/Communication Waiting (CW)

D.5.1 Procedures

D.5.1.1 Activation

(wait for dial tone) *43# (wait for ack.)

(wait for dial tone) *43*0# (wait for ack.) (for all VoIP lines)

D.5.1.2. Deactivation

(wait for dial tone) #43# (wait for ack.)

(wait for dial tone) #43*0# (wait for ack.) (for all VoIP lines)

D.5.1.3 Interrogation

(wait for dial tone) *#43# (wait for ack.)

D.5.1.4 Invocation

D.5.1.4.1 Acceptance of an incoming communication (with or without authorisation of 3PTY service)

(hang-up and wait for ringing signal)

D.5.1.4.2 Acceptance of an incoming communication (with authorisation of 3PTY service)

a) (wait for special dial tone) **1** (the current communication will be released)

b) (wait for special dial tone) **2** (the current communication is put on HOLD)

D.5.1.4.3 Rejection of an incoming communication

(wait for special dial tone) **0** (the incoming communication will be rejected)

Annex D.6 HOLD / TOGGLE

D.6.1 Procedures

D.6.1.1 Invocation (…)

(wait for special dial tone and dial third party number) <DN> (0…9)

D.6.1.1.1 Worst case (communication could not be established)

a) (wait for special dial tone) **1**

b) (hang-up and wait for ringing signal)

D.6.1.2 Invocation (change to the party on HOLD –TOGGLE-)

(wait for special dial tone) **2** (the current communication is put on HOLD)

D.6.1.3 Invocation (release a communication during HOLD)

D.6.1.3.1 Invocation (release the current communication)

(wait for special dial tone) **1** (the communication on HOLD becomes active)

D.6.1.3.2 Invocation (release the communication on HOLD)

(wait for special dial tone) **0** (the communication on HOLD will be released)

D.6.1.3 Invocation (Release initiated by the current party)

Congestion tone provided

(wait for special dial tone) **1** or **2** or

(wait for ringing tone)

Annex D.7 Three Party Conference/Conference (3PTY/CONF)

D.7.1 Procedures

D.7.1.1 Invocation (3PTY/CONF initiation)

Prerequisite: Initiator has one communication in an active state and a second communication on hold.

(wait for special dial tone) **3**

D.7.1.2 Invocation (change from 3PTY/CONF to HOLD/TOGGLE)

(wait for special dial tone) **2**

Annex D.8 Communication Diversion: Call Forwarding Unconditional / Communication Forwarding Unconditional (CDIV:CFU)

D.8.1 Procedures

D.8.1.1 Activation [1]

D.8.1.1.1 Activation without Call Forwarded Number (CFN)

(wait for dial tone) *21# (wait for ack.) [2]

D.8.1.1.2 Activation with CFN

(wait for dial tone) *21*<CFN># (wait for ack.)

D.8.1.2 Deactivation

(wait for dial tone) #21# (wait for ack.)

1 While CFU is activated the special dial tone shall be played after picking up the receiver instead of normal dial tone to remember the user that no incoming calls will be received.

2 CFN has already been registered before.

D.8.1.3 Delete / Reset

(wait for dial tone) ##21# (wait for ack.) [1]

D.8.1.4 Interrogation

(wait for dial tone) *#21# (wait for ack.)

Annex D.9 Communication Diversion: Call Forwarding Busy / Communication Forwarding Busy (CDIV:CFB)

D.9.1 Procedures

D.9.1.1 Activation

D.9.1.1.1 Activation without Call Forwarded Number (CFN)

(wait for dial tone) *67# (wait for ack.) [1]

D.9.1.1.2 Activation with CFN

(wait for dial tone) *67*<CFN># (wait for ack.)

D.9.1.2 Deactivation

(wait for dial tone) #67# (wait for ack.)

D.9.1.3 Delete / Reset

(wait for dial tone) ##67# (wait for ack.) [2]

D.9.1.4 Interrogation

(wait for dial tone) *#67# (wait for ack.)

---

[1] After Delete/Reset the current CFU is deactivated and the default CFU is set automatically according to the initial configuration of this VoIP line.

[2] After Delete/Reset the current CFB/CFNR is deactivated and the default CFB/CFNR is set automatically according to the initial configuration of this VoIP line; In case of CFNR the timer value is set to 20 seconds (default).

Annex D.10 Communication Diversion: Call Forwarding No Reply/ Communication Forwarding No Reply (CDIV:CFNR)

D.10.1 Procedures

D.10.1.1 Activation

D.10.1.1.1 Activation without Call Forwarded Number (CFN) and without timer value

(wait for dial tone) *61# (wait for ack.) [1] [2]

D.10.1.1.2 Activation with CFN; and without timer value

(wait for dial tone) *61*<CFN># (wait for ack.)

D.10.1.1.3 Activation with CFN and with timer value [3]

(wait for dial tone) *61*<CFN>*<timer value># (wait for ack.)

D.10.1.1.4 Activation and modification of timer value (without CFN) [1]

(wait for dial tone) *61**<timer value># (wait for ack.) [1]

D.10.1.2 Deactivation

(wait for dial tone) #61# (wait for ack.)

D.10.1.3 Delete / Reset

(wait for dial tone) ##61# (wait for ack.) [1]

D.10.1.4 Interrogation

(wait for dial tone) *#61# (wait for ack.)

---

[1] CFN has already been registered before.

[2] Default timer value or timer value has already been registered before.

[3] The timer value has a valid range from 5 to 60 (seconds) in steps of 1 (second); default value is 20 seconds; the timer value item may consist of 1 or 2 digits; in case of an invalid entry the current timer value is kept unchanged.

Annex D.11 Communication Diversion: Selective Call Forwarding Unconditional/ Selective Communication Forwarding Unconditional (CDIV:S-CFU)

D.11.1 Procedures

D.11.1.1 Activation [1]

(wait for dial tone) *212*<CFN>*<ON[2]># (wait for ack.)

D.11.1.2 Deactivation

(wait for dial tone) #212# (wait for ack.)

or

(wait for dial tone) #212*<ON># (wait for ack.)

D.11.1.3 Delete / Reset

(wait for dial tone) ##212# (wait for ack.) [3]

D.11.1.4 Interrogation

(wait for dial tone) *#212# (wait for ack.)

Annex D.12 Communication Diversion: Selective Call Forwarding Busy/ Selective Communication Forwarding Busy (CDIV:S-CFB)

D.12.1 Procedures

D.12.1.1 Activation

(wait for dial tone) *214*<CFN>*<ON># (wait for ack.)

D.12.1.2 Deactivation

(wait for dial tone) #214# (wait for ack.)

---

[1] While S-CFU is activated the special dial tone shall be played after picking up the receiver instead of normal dial tone to remember the user that no incoming calls will be received.

[2] ON= Originating Number

[3] After Delete/Reset the current S-CFU is deactivated and the default S-CFU is set automatically according to the initial configuration of this VoIP line.

or

(wait for dial tone) #214*<ON># (wait for ack.)

D.12.1.3 Delete / Reset

(wait for dial tone) ##214# (wait for ack.) [1]

D.12.1.4 Interrogation

(wait for dial tone) *#214# (wait for ack.)

Annex D.13 Communication Diversion: Selective Call Forwarding No Reply/ Selective Communication Forwarding No Reply (CDIV:S-CFNR)

D.13.1 Procedures

D.13.1.1 Activation

D.13.1.1.1 Activation with CFN and without timer value

(wait for dial tone) *213*<CFN>*<ON># (wait for ack.) [2]

D.13.1.1.2 Activation with CFN and with timer value [3]

(wait for dial tone) *213*<CFN>*<ON>*<timer value># (wait for ack.)

D.13.1.2 Deactivation

(wait for dial tone) #213# (wait for ack.)

or

(wait for dial tone) #213*<ON># (wait for ack.)

D.13.1.3 Delete / Reset

(wait for dial tone) ##213# (wait for ack.) [1]

---

[1] After Delete/Reset the current S-CFB/S-CFNR is deactivated and the default S-CFB/S-CFNR is set automatically according to the initial configuration of this VoIP line; In case of S-CFNR the timer value is set to 20 seconds (default).

[2] Default timer value or timer value has already been registered before.

[3] The timer value has a valid range from 5 to 60 (seconds) in steps of 1 (second); default value is 20 seconds; the timer value item may consist of 1 or 2 digits; in case of an invalid entry the current timer value is kept unchanged.

D.13.1.4 Interrogation

(wait for dial tone) *#213# (wait for ack.)

Annex D.14 Selective Call Forwarding/ Selective Communication Forwarding – Deletion/Reset

D.14.1 Procedures

D.14.1.1 Activation

Not applicable.

D.14.1.2 Deactivation

Not applicable.

D.14.1.3 Delete/Reset

(wait for dial tone) #211# (wait for ack.) [1]

or

(wait for dial tone) #211*0# (wait for ack.) (for all VoIP lines) [1]

D.14.1.4 Interrogation

Not applicable.

Annex D.15 Communication Forwarding on Not Logged-in (CFNL)

D.15.1 Procedures

D.15.1.1 Activation

D.15.1.1.1 Activation without Call Forwarding Number (CFN)

(wait for dial tone) *62# (wait for ack.) [2]

D.15.1.1.2 Activation with CFN

(wait for dial tone) *62*<CFN># (wait for ack.)

D.15.1.2Deactivation

---

[1] After Delete/Reset all current S-CF features are deactivated and all default S-CF features are set automatically according to the initial configuration of this VoIP line; The timer value (S-CFNR) is set to 20 seconds (default).

[2] CFN has already been registered before.

(wait for dial tone) #62# (wait for ack.)

D.15.1.3 Delete / Reset

(wait for dial tone) ##62# (wait for ack.) [1]

D.15.1.4 Interrogation

(wait for dial tone) *#62# (wait for ack.)

Annex D.15A Communication Forwarding (time controlled)

D.15A.1 Procedures

D.15A.1.1 Activation

(wait for dial tone) *621# (wait for ack.)

Activation with traget

(wait for dial tone) *621*<target># (wait for ack.)

D.15A.1.2 Deactivation

(wait for dial tone) #621# (wait for ack.)

Annex D.16 Communication Barring - Incoming Communication Barring (ICB)

D.16.1 Procedures

D.16.1.1 Activation

(wait for dial tone) *335*<PIN># (wait for ack.)

(wait for dial tone) *335*<PIN>*0# (wait for ack.) (for all VoIP lines)

D.16.1.2 Deactivation

(wait for dial tone) #335*<PIN># (wait for ack.)

(wait for dial tone) #335*<PIN>*0# (wait for ack.) (for all VoIP lines)

D.16.1.3 Interrogation

(wait for dial tone) *#335# (wait for ack.)

[1] After Delete/Reset the current CFNL is deactivated and the default CFNL is set automatically according to the initial configuration of this VoIP line.

Annex D.17 Communication Barring - Forwarded Communication Barring

D.17.1 Procedures

D.17.1.1 Activation

(wait for dial tone) *337*<PIN># (wait for ack.)

(wait for dial tone) *337*<PIN>*0# (wait for ack.) (for all VoIP lines)

D.17.1.2 Deactivation

(wait for dial tone) #337*<PIN># (wait for ack.)

(wait for dial tone) #337*<PIN>*0# (wait for ack.) (for all VoIP lines)

D.17.1.3 Interrogation

(wait for dial tone) *#337# (wait for ack.)

Annex D.18 Communication Barring - Anonymous Communication Rejection (ACR)

D.18.1 Procedures

D.18.1.1 Activation

(wait for dial tone) *336*<PIN># (wait for ack.)

(wait for dial tone) *336*<PIN>*0# (wait for ack.) (for all VoIP lines)

D.18.1.2 Deactivation

(wait for dial tone) #336*<PIN># (wait for ack.)

(wait for dial tone) #336*<PIN>*0# (wait for ack.) (for all VoIP lines)

D.18.1.3 Interrogation

(wait for dial tone) *#336# (wait for ack.)

Annex D.19 Communication Barring – Incoming Communication Barring: White list

D.19.1 Procedures

D.19.1.1 Activation “White List” without Calling Number (CN)

(wait for dial tone) *339*<PIN># (wait for ack.)

(wait for dial tone) *339*<PIN>**0# (wait for ack.) (for all VoIP lines)

D.19.1.2 Activation “White List” with Calling Number (CN)

(wait for dial tone) *339*<PIN>*<CN># (wait for ack.)

(wait for dial tone) *339*<PIN>*<CN>*0# (wait for ack.) (for all VoIP lines)

D.19.1.3 Deactivation

(wait for dial tone) #339*<PIN># (wait for ack.)

(wait for dial tone) #339*<PIN>*0# (wait for ack.) (for all VoIP lines)

D.19.1.4 Delete White list

(wait for dial tone) ##339*<PIN># (wait for ack.)

(wait for dial tone) ##339*<PIN>*0# (wait for ack.) (for all VoIP lines)

D.19.1.5 Interrogation

(wait for dial tone) *#339# (wait for ack.)

Annex D.20 Communication Barring – Incoming Communication Barring: Black list

D.20.1 Procedures

D.20.1.1 Activation “Black List” without Calling Number (CN)

(wait for dial tone) *338*<PIN># (wait for ack.)

(wait for dial tone) *338*<PIN>**0# (wait for ack.) (for all VoIP lines)

D.20.1.2 Activation “Black List” with Calling Number (CN)

(wait for dial tone) *338*<PIN>*<CN># (wait for ack.)

(wait for dial tone) *338*<PIN>*<CN>*0# (wait for ack.) (for all VoIP lines)

D.20.1.3 Deactivation

(wait for dial tone) #338*<PIN># (wait for ack.)

(wait for dial tone) #338*<PIN>*0# (wait for ack.) (for all VoIP lines)

D.20.1.4 Delete Black list

(wait for dial tone) ##338*<PIN># (wait for ack.)

(wait for dial tone) ##338*<PIN>*0# (wait for ack.) (for all VoIP lines)

D.20.1.5 Interrogation

(wait for dial tone) *#338# (wait for ack.)

Annex D.21 Communication Barring –Incoming Communication Barring: Virtual Black list / Kick Out

D.21.1 Procedures

D.21.1.1 Activation

(wait for dial tone) *934*<PIN># (wait for ack.)

D.21.1.2 Activation/Deactivation (toggle mode)

(wait for dial tone) #934*<PIN># (wait for ack.)

D.21.1.3 Delete virtual Black list

(wait for dial tone) ##934*<PIN># (wait for ack.)

D.21.1.4 Interrogation

(wait for dial tone) *#934# (wait for ack.)

Annex D.22 Communication Barring - Outgoing Communication Barring (OCB)

D.22.1 Procedures

D.22.1.1 Activation

D.22.1.1.1 Outgoing Communications - All

(wait for dial tone) *03*<PIN># (wait for ack.)

D.22.1.1.2 Outgoing Communications - Selective

(wait for dial tone) *05*<PIN># (wait for ack.) (for all activated classes)

D.22.1.1.2.1 Selective Outgoing Communications to 0900 …

(wait for dial tone) *051*<PIN># (wait for ack.)

D.22.1.1.2.2 Selective Outgoing Communications to 0137 …

(wait for dial tone) *052*<PIN># (wait for ack.)

D.22.1.1.2.3 Selective Outgoing Communications to 0180 …

(wait for dial tone) *053*<PIN># (wait for ack.)

D.22.1.1.2.4 Selective Outgoing Communications to International numbers (00)

(wait for dial tone) *054*<PIN># (wait for ack.)

D.22.1.1.2.5 Selective Outgoing Communications to Intercontinental numbers (0011-0019, 002, 005-009)

(wait for dial tone) *055*<PIN># (wait for ack.)

D.22.1.2. Deactivation

D.22.1.2.1 Outgoing Communications - All

(wait for dial tone) #03*<PIN># (wait for ack.)

D.22.1.2.2 Outgoing Communications - Selective

(wait for dial tone) #05*<PIN># (wait for ack.) (for all activated classes)

D.22.1.2.2.1 Selective Outgoing Communications to 0900 …

(wait for dial tone) #051*<PIN># (wait for ack.)

D.22.1.2.2.2 Selective Outgoing Communications to 0137 …

(wait for dial tone) #052*<PIN># (wait for ack.)

D.22.1.2.2.3 Selective Outgoing Communications to 0180 …

(wait for dial tone) #053*<PIN># (wait for ack.)

D.22.1.2.2.4 Selective Outgoing Communications to International numbers (00)

(wait for dial tone) #054*<PIN># (wait for ack.)

D.22.1.2.2.5 Selective Outgoing Communications to Intercontinental numbers (0011-0019, 002, 005-009)

(wait for dial tone) #055*<PIN> # (wait for ack.)

D.22.1.3 Interrogation

D.22.1.3.1 All Outgoing Communications

(wait for dial tone) *#03# (wait for ack.)

D.22.1.3.2 Selective Outgoing Communications

(wait for dial tone) *#05# (wait for ack.)

Annex D.23 Communication Barring –Outgoing Communication Barring: White list

D.23.1 Procedures

D.23.1.1 Activation “White List” without Originating Number (ON)

(wait for dial tone) *04*<PIN># (wait for ack.)

D.23.1.2 Activation “White List” with Originating Number (ON)

(wait for dial tone) *04*<PIN>*<ON># (wait for ack.)

(wait for dial tone) *04*<PIN>*<ON>*0# (wait for ack.) (for all VoIP lines)

D.23.1.3 Deactivation

(wait for dial tone) #04*<PIN># (wait for ack.)

D.23.1.4 Delete White list

(wait for dial tone) ##04*<PIN># (wait for ack.)

(wait for dial tone) ##04*<PIN>*0# (wait for ack.) (for all VoIP lines)

D.23.1.5 Interrogation

(wait for dial tone) *#04# (wait for ack.)

Annex D.24 Communication Barring – Outgoing Communication Barring: Black list

D.24.1 Procedures

D.24.1.1 Activation "Black List" without Originating Number (ON)

(wait for dial tone) *059*<PIN># (wait for ack.)

D.24.1.2 Activation "Black List" with Originating Number (ON)

(wait for dial tone) *059*<PIN>*<ON># (wait for ack.)

(wait for dial tone) *059*<PIN>*<ON>*0# (wait for ack.) (for all VoIP lines)

D.24.1.3 Deactivation

(wait for dial tone) #059*<PIN># (wait for ack.)

D.24.1.4 Delete Blacklist

(wait for dial tone) ##059*<PIN># (wait for ack.)

(wait for dial tone) ##059*<PIN>*0# (wait for ack.) (for all VoIP lines)

D.24.1.5 Interrogation

(wait for dial tone) *#059# (wait for ack.)

Annex D.25 Completion of Communication to Busy Subscriber (CCBS)

D.25.1 Procedures

D.25.1.1 Activation

(subscriber busy; announcement CCBS possible) *37# (wait for ack.)

D.25.1.2. Deactivation of all activated recalls

(wait for dial tone) #37# (wait for ack.)

D.25.1.3 Interrogation

(wait for dial tone) *#37# (wait for ack.)

Annex D.26 Completion of Communication on No Reply (CCNR)

D.26.1 Procedures

D.26.1.1 Activation

(announcement CCNR possible) *38# (wait for ack.)

D.26.1.2. Deactivation of all activated recalls

(wait for dial tone) #38# (wait for ack.)

D.26.1.3 Interrogation

(wait for dial tone) *#38# (wait for ack.)

Annex D.27 Completion of Communication on Not Logged-in (CCNL)

D.27.1 Procedures

D.27.1.1 Activation

(no answer; announcement CCNL possible) *36# (wait for ack.)

D.27.1.2. Deactivation

(wait for dial tone) #36# (wait for ack.)

D.27.1.3 Interrogation

(wait for dial tone) *#36# (wait for ack.)

Annex D.28 Void

Annex D.29 PIN Modification

D.29.1 Procedures

D.29.1.1 PIN modification

(wait for dial tone) *99*<PINold>*<PINnew>*<PINnew># (wait for ack.)

Annex D.30 Reset All Services to Default Values

D.30.1 Procedures

D.30.1.1 Activation

D.30.1.1.1 Activation without deletion of list entries

(wait for dial tone) *001*<PIN># (wait for ack.)

or

(wait for dial tone) *001*<PIN>*0# (wait for ack.) (for all VoIP lines)

D.30.1.1.2 Activation with deletion of list entries

(wait for dial tone) *000*<PIN># (wait for ack.)

or

(wait for dial tone) *000*<PIN>*0# (wait for ack.) (for all VoIP lines)

D.30.1.2. Deactivation

Not applicable.

D.30.1.3 Interrogation

Not applicable.

Annex D.31 Malicious Communication Identification

D.31.1 Procedures

D.31.1.1 Activation

(wait for dial tone) *39# (wait for ack.) (flag the last call)

(wait for dial tone) *392# (wait for ack.) (flag the penultimate call)

D.31.1.2. Deactivation

Not applicable.

D.31.1.3 Interrogation

Not applicable.

Annex E (informative) Supervisory tones

Annex E.0 General

This annex E provides user equipment information (e.g. for SIP phones) with the purpose to optimise the user interface by generating the well known supervisory tones in the UE.

The following tables provide the respective audible tones according to the relevant cause:

Cause	Audible tone
Off-hook; as prescribed in user profile: name= „dial-tone-pattern“ (default = „standard-dial-tone“).	Dial tone
Like „Dial tone“; as prescribed in user profile: name= „dial-tone-pattern“, value = „special-condition-tone“.	Special dial tone
SIP INVITE request with CW indication during communication state.	Communication waiting tone
Receipt of a SIP response “180 Ringing” without P-Early-Media header.	Ringing tone
Receipt of a SIP response “486 Busy Here”	Busy tone
After receipt of any 4xx, 5xx or 6xx responses as well as on receipt of a BYE or CANCEL request in off-hook or communication state.	Congestion tone

Table Annex E 1: Audible tones

Responses with Reason-Header, cause = [1]		Audible tone
16	„Normal call clearing“	Congestion tone
17	„User busy“	Busy tone
18	„No user responding“	Busy tone
19	„No answer from user (user alerted)”	Busy tone
28	„Address incomplete“	Congestion tone
31	„Normal, unspecified“	Congestion tone
34	„No circuit/ channel available“	Congestion tone
38	„Network out of order“	Congestion tone
41	„Temporary failure“	Congestion tone
44	„Requested circuit/channel not available”	Congestion tone
47	„Resources unavailable, unspecified”	Congestion tone
58	„Bearer capability not implemented“	Congestion tone
91	„Invalid transit selection“	Congestion tone
102	„Recovery on timer expiry“	Congestion tone

[1] Causes according to Q.850. On deviant cause values the “Congestion tone” shall be played.
If the Reason header is missing, the audible tone regarding the SIP response/request (upper part of Table Annex E 1) shall be played.

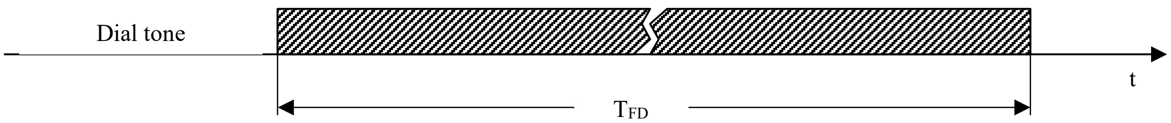
Responses with Reason-Header, cause = [1]	Audible tone
127 „Interworking unspecified“	Congestion tone

The levels for audible tones shall be properly defined. The following signals should be provided by a UE.

Annex E.1 Dial tone

The dial tone should be applied in the off-hook state (receiver picked up or loudspeaker activated) until the first digit has been dialled. It serves as information “ready for dialling” for the subscriber or specific terminal devices.

The dial tone should be a permanent tone with a frequency range of 425 Hz ± 7 Hz and a distortion factor of k ≤ 5 % as depicted in the figure below.

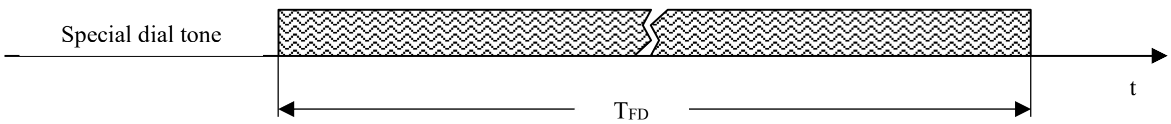


Annex E.2 Special dial tone

The special dial tone should be applied in the off-hook state (receiver picked up or loudspeaker activated) in conjunction with a particular case (e.g. CFU is activated) until the first digit has been dialled. It serves as information “ready for dialling” for the subscriber or specific terminal devices.

In addition, the special dial tone gives the subscriber a hint about a specific situation (e.g. another party is on hold).

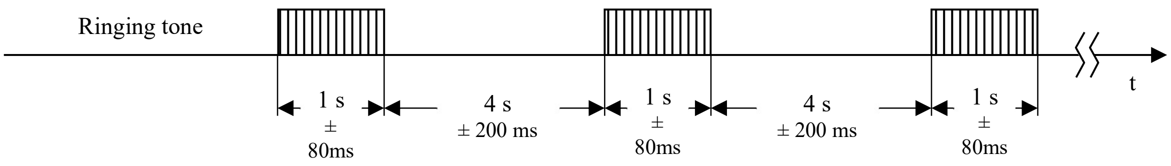
The special dial tone should be a permanent tone with a frequency composition range of f_1 = 400 Hz ± 7 Hz and f_2 = 425 Hz ± 7 Hz (additive); the distortion factor shall be k ≤ 5 % as depicted in the figure below.



Annex E.3 Ringing tone

The ringing tone is provided after a successful communication set-up is finalized and the destination party is idle. The ringing tone serves as information “ringing signal is provided to the destination party” for the subscriber or specific terminal devices.

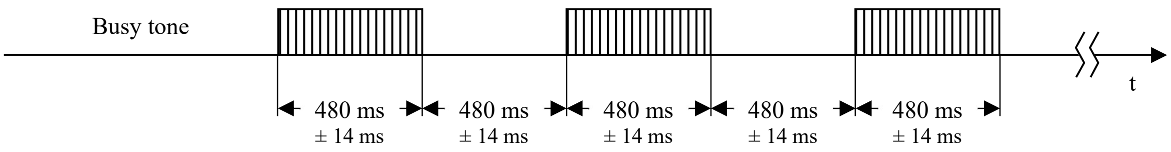
The ringing tone should be a paced tone with a frequency range of 425 Hz ± 7 Hz and a distortion factor of k ≤ 5 % as depicted in the figure below.



Annex E.4 Busy tone

The busy tone is provided after a successful communication set-up is finalized and the destination party is busy. The busy tone serves as information “destination party busy” for the subscriber or specific terminal devices.

The busy tone should be a paced tone with a frequency range of 425 Hz ± 7 Hz and a distortion factor of k ≤ 5 % as depicted in the figure below.



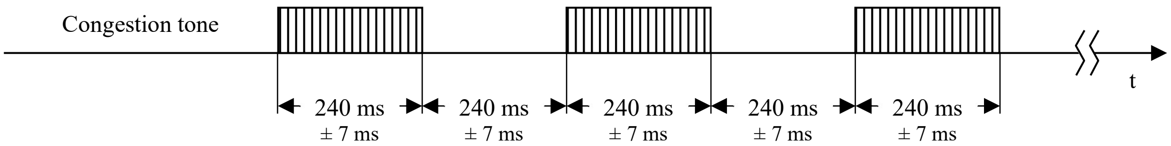
Annex E.5 Congestion tone

The congestion tone is provided in case of an unsuccessful communication set-up or in case of an error. The congestion tone serves as information “unsuccessful communication” or “operating error” (see bullet points below) for the subscriber or specific terminal devices.

The congestion tone should be a paced tone with a frequency range of 425 Hz ± 7 Hz and a distortion factor of k ≤ 5 % as depicted in the figure below.

The congestion tone is played in case the following causes:

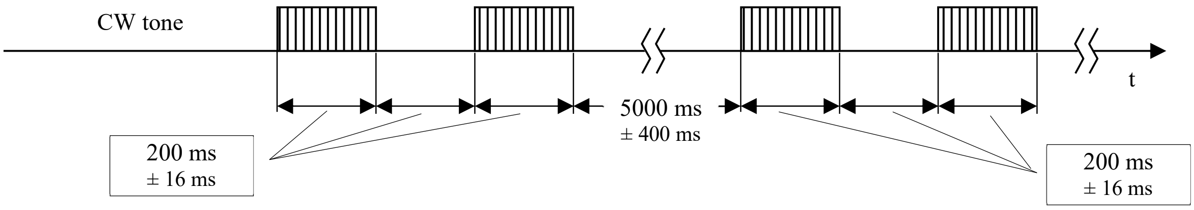
- Communication set-up to the destination party is not possible,
- a time-out has expired,
- a garbage has been detected (e.g. SOC/SCC).



Annex E.6 Communication waiting tone

The communication waiting tone (CW tone) is provided during the communication state while a third party communication is waiting. The CW tone serves as information "another communication is waiting" for the subscriber or specific terminal devices.

The communication waiting tone should be a paced tone with a frequency range of 425 Hz ± 7 Hz and a distortion factor of k ≤ 5 % as depicted in the figure below.



Annex E.7 Acoustic ringing signal

The acoustic ringing signal for incoming calls (external call) is provided during the idle state and should have the following ringing cadence:

Table E.7-1

	Duration in ms				
Ringing signal (pulse)	920	≤	1000	≤	1080
Ringing signal pause	4800	≤	5000	≤	5200

Additional deviated ringing cadences for other kind of calls or features are possible.

ANNEX F Implementation example of DNS Procedures (Informative)

For DNS procedures the baseline 1TR114 Annex B is valid (Section ANNEX E)

F.1 VoSIP related DNS

Regarding VoIP communication the UE typically requests URI's like following (non-exhaustive):

- sip:tel.t-online.de (Register)
- sip:user@tel.t-online.de (Invite)

Thereafter VoSIP compliant UE's/IAD request NAPTR records for the requested (example) domain "tel.t-online.de"

Standard query

Queries

tel.t-online.de: type NAPTR, class IN

Standard query response

Answers

tel.t-online.de. IN NAPTR 50 50 "s" "SIPS+D2T" _sips._tcp.tel.t-online.de.

tel.t-online.de. IN NAPTR 90 50 "s" "SIP+D2U" _sip._udp.tel.t-online.de.

tel.t-online.de. IN NAPTR 100 50 "s" "SIP+D2T" _sip._tcp.tel.t-online.de.

After receipt of the DNS NAPTR response the UE must execute the entries according standards (RFCs 3263, 3401, 3402, 3403, 3404 etc.)

The IMS platform of Deutsche Telekom is responsible for the order of preference of the records within the DNS NAPTR response.

If the DNS server response contains multiple NAPTR records, the UE must discard any records which are not applicable.

In case the UE requested a SIP URI, if the DNS NAPTR response contains records with 'SIPS' as protocol this must be retained by the UE acc. to RFC 3263.

Which record finally is used depends therefore both on:

- UE: supported protocols by the UE (for VoSIP compliant UE's: 'TLS over TCP' or 'UDP') and
- VoIP core: the order of preference by the platform servers (according to the ranking in the NAPTR response)

F.2 Example VoSIP DNS message flow

Standard query

Queries

tel.t-online.de: type NAPTR, class IN

Standard query response

Answers

tel.t-online.de. IN NAPTR 50 50 "s" "SIPS+D2T" _sips._tcp.tel.t-online.de.

tel.t-online.de. IN NAPTR 90 50 "s" "SIP+D2U" _sip._udp.tel.t-online.de.

tel.t-online.de. IN NAPTR 100 50 "s" "SIP+D2T" _sip._tcp.tel.t-online.de.

Standard query

Queries

_sips._tcp.tel.t-online.de: type SRV, class IN

Standard query response

Answers

_sips._tcp.tel.t-online.de: type SRV, class IN, priority 0, weight 5, port 5061, target tas001.voip.t-ipnet.de

sips._tcp.tel.t-online.de: type SRV, class IN, priority 1, weight 5, port 5061, target tas002.voip.t-ipnet.de

Additional records

tas001.voip.t-ipnet.de: type A, class IN, addr 217.1.1.1

tas002.voip.t-ipnet.de: type A, class IN, addr 217.1.1.2

Example DNS sequence diagrams

- Successful DNS query for secure _sips._tcp

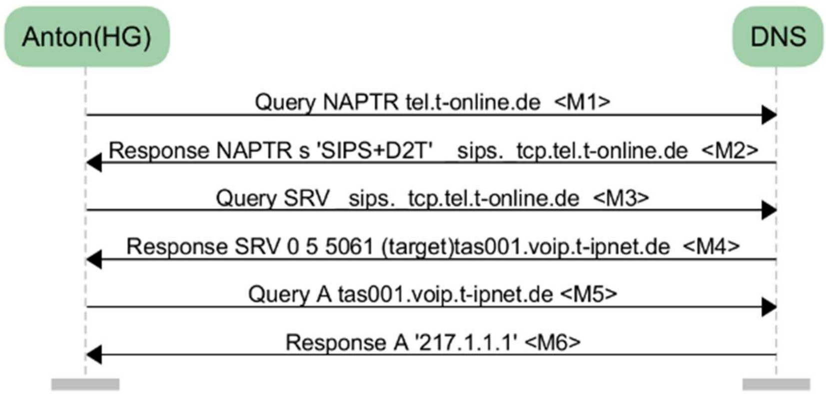


Figure F2.1 successful DNS (SIPS)

ANNEX G Early Media (normative)

G.1 Methodology

G.1.1 Expressions/Variables used

G.1.1.1 Dialog-ID

The Dialog-ID in this ANNEX is the dialog identifier as defined in RFC3261 [26] section 12:

For a UAC, the Call-ID value of the dialog ID is set to the Call-ID of the message, the remote tag is set to the tag in the To field of the message, and the local tag is set to the tag in the From field of the message (these rules apply to both requests and responses)

G.1.1.2 Status_Change

Status_Change returns a value which indicates if the status of the early dialog "X" has been changed The Value of Status_Change is set and changed in procedure "Check_SDP_P-Early-media_180".The value of Status_Change is either "FALSE" or "TRUE"

G.1.1.3 MEDIA_CTRL_Dialog

MEDIA_CTRL_Dialog has either the value "none" if no early dialog is established or "X" which reflects the dialog identifier (Dialog-ID) of the early dialog.

G.1.1.4 Message

Message will take the name of the current received SIP Message (e.G. 180 (Ringing), 183 (Progress), 199(Early Dialog Terminated), UPDATE...).

G.1.1.5 P-Early-Media (X)

P-Early-Media (X) will be stored and used per early dialog "X", P-Early-Media (X) can have the values "none", "sendonly", "sendrecv", "recvonly" or "inactive",In Check_SDP_P-Early-Media_180 "none" is used to initialize P-Early-Media (X) when a new dialog is in process. The values "sendonly", "sendrecv", "recvonly" or "inactive" are set accordingly to the value received within the SIP P-Early-Media Header field. The value "sendonly" is also used as default value when SDP is available and no SIP P-Early-Media Header is received.

G.1.1.6 180(X)

180 (X) will be stored and used per early dialog "X", 180 (X) can have the values "TRUE" when 180 for dialog "X" is received and "FALSE" if not

G.1.1.7 SDP(X)

SDP (X) will be stored and used per early dialog "X", SDP (X) can have the values "TRUE" when SDP for dialog "X" is received and "FALSE" if not

G.1.1.8 Timer_RTP

Timer_RTP is initialized with the start value of the timer and decreasing till zero until observing if RTP is received by the IAD.

G.1.2 Procedures used

G.1.2.1 Check_SDP_P-Early-Media_180

This procedure evaluates and/or set the values of "Status_Change", "P-Early-Media (X)", "180 (X)" and "SDP (X)"

The variable "X" refers to the Dialog-ID

The procedure "Check_SDP_P-Early-Media_180" checks the status as follows:

- if protocol elements of the SIP P-Early-Media header field regarding RFC 5009 [109] are received,
- if the response value 180 (Ringing) is received, and
- if an RFC3264 [27B] conformant SDP answer is available.

G.1.2.2 Process_Message

This procedure is the normal call processing regarding the procedures described in 1TR114 except handling of early-media & local ring-tone which is described within this Document.

G.1.3 States

G.1.3.1 ED_NoMedia

Is the state where media is neither received nor generated and rendered to the user.

G.1.3.2 ED_LocalRingtone

Is the state where a local ringback tone is generated and rendered to the user.

G.1.3.3 ED_EarlyMedia

Is the state where the early dialog indicates that early media is received and is rendered to the user.
Due to some use cases this state may change to ED_LocalRingtone when RTP is not received and a 180 (Ringing) was received.
In other cases, the user will not hear anything where no RTP is available and no 180 (Ringing) was received.

G.1.3.4 Wait_EM

This state waits for any SIP message received by the IAD.

G.2 SDL Diagrams for Early Media Handling

G.2.1 State Idle & State Wait_EarlyMedia

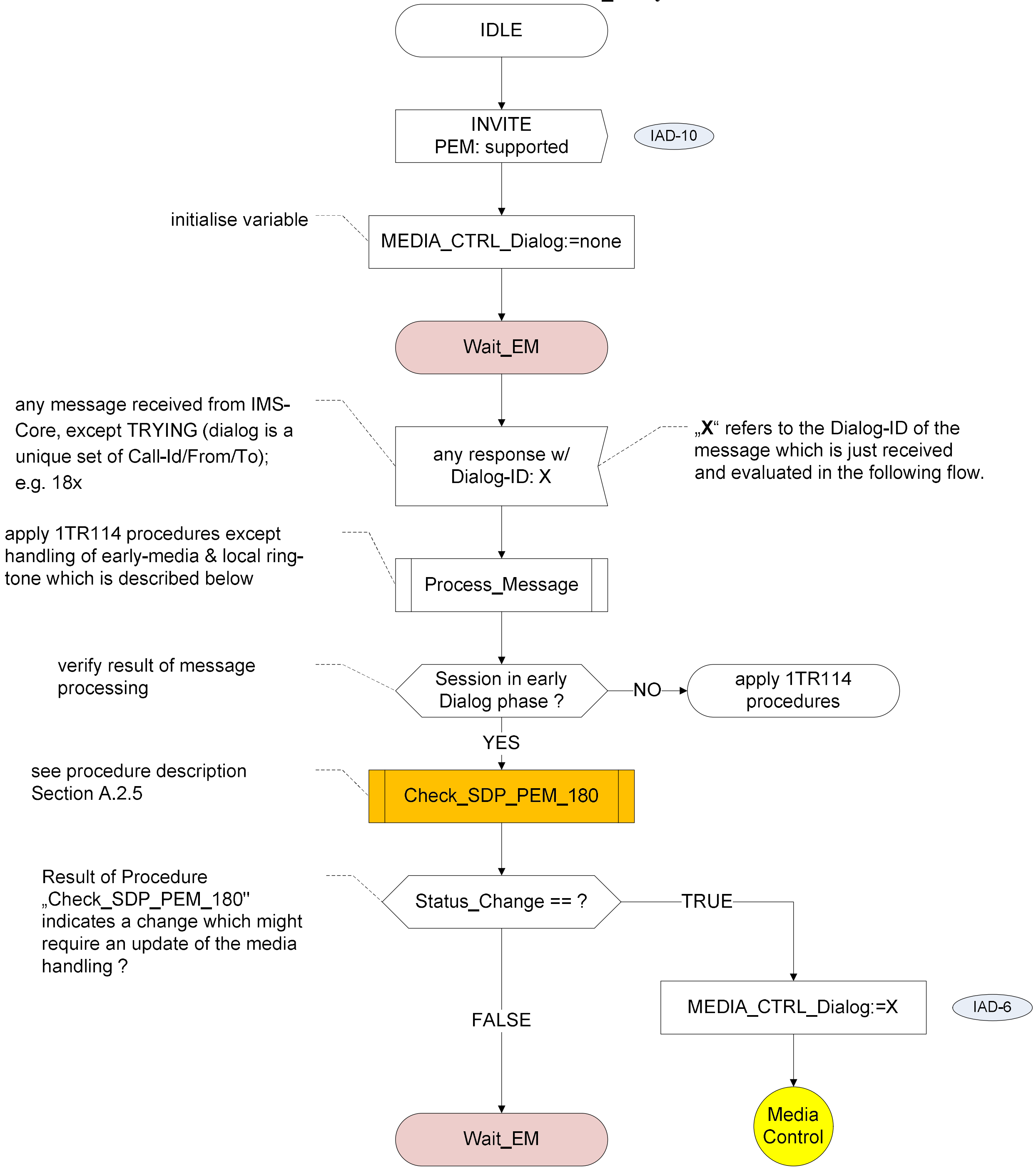


Figure G.2.1.1: State Idle & State Wait_EarlyMedia

G.2.2 Media Control

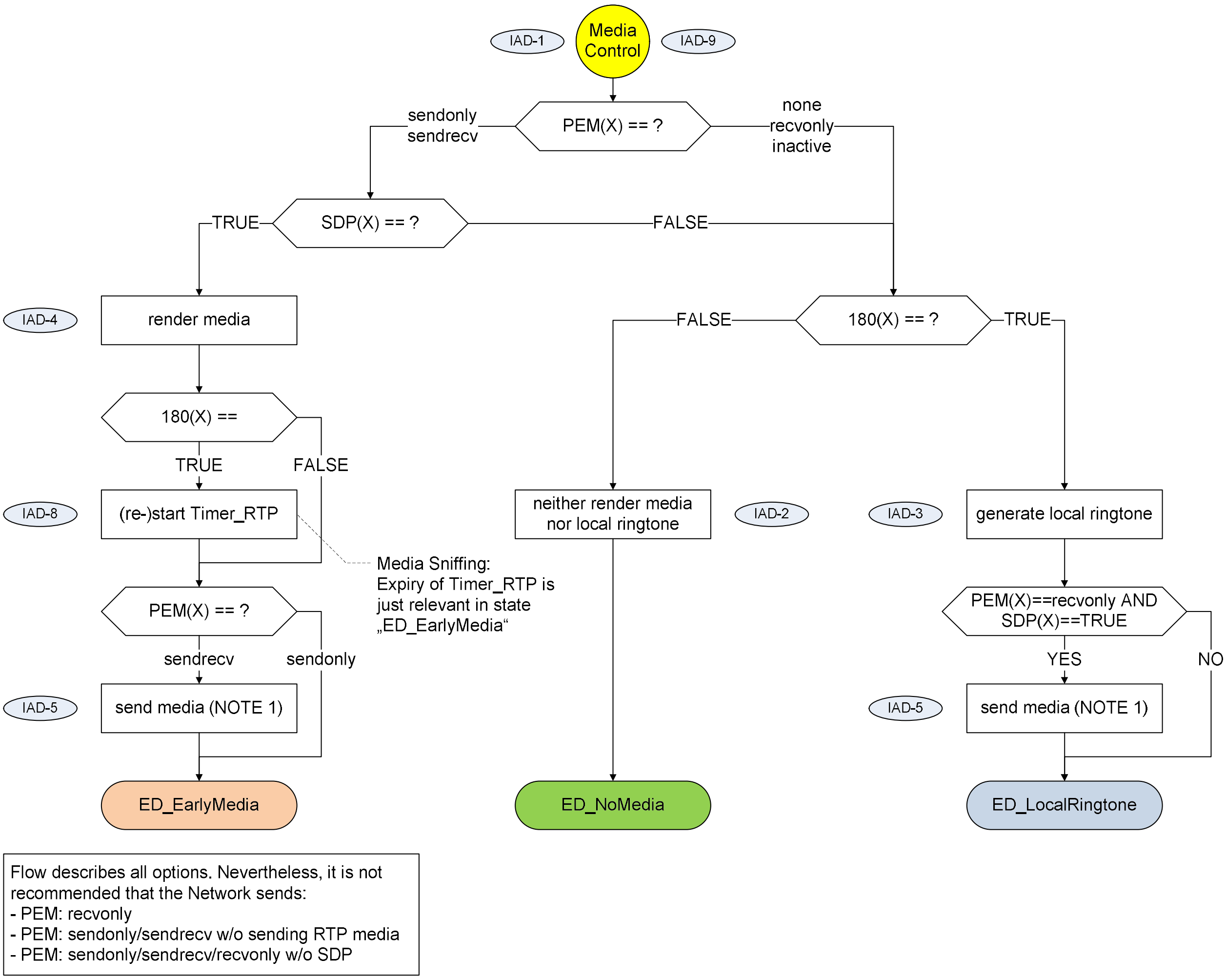


Figure G.2.2.1 Media Control

G.2.3 State EarlyDialog_NoMedia (ED_NoMedia)

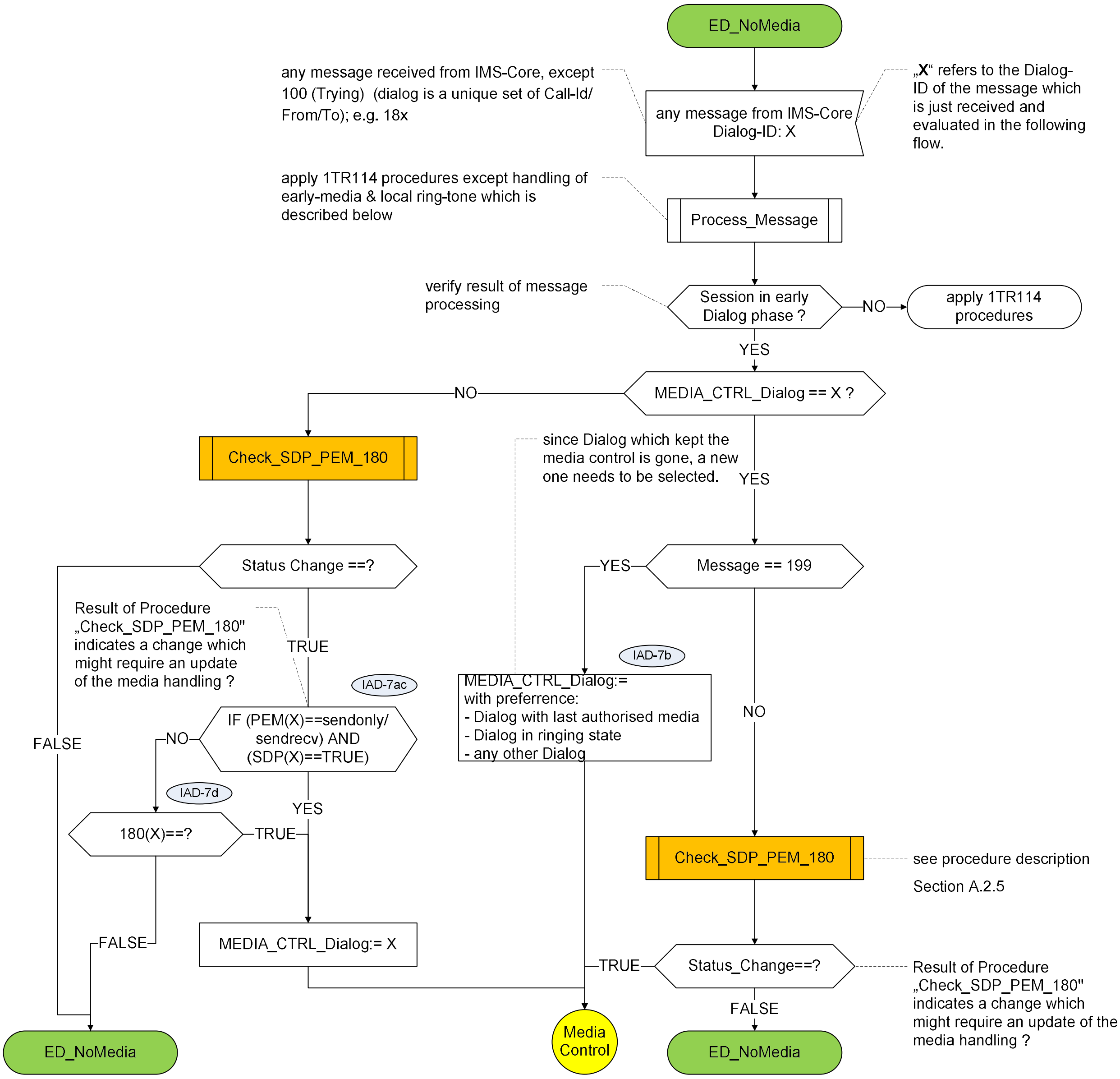


Figure G.2.3.1:State EarlyDialog_NoMedia

G.2.4 State EarlyDialog_EarlyMedia (ED_EarlyMedia) & State EarlyDialog_LocalRingtone (ED_LocalRingtone)

Process as shown in Figure G.2.4.1 is running in parallel when the state ED_EarlyMedia is applying. In cases the state changes due to other procedures to another state then the timer expiry is ignored.

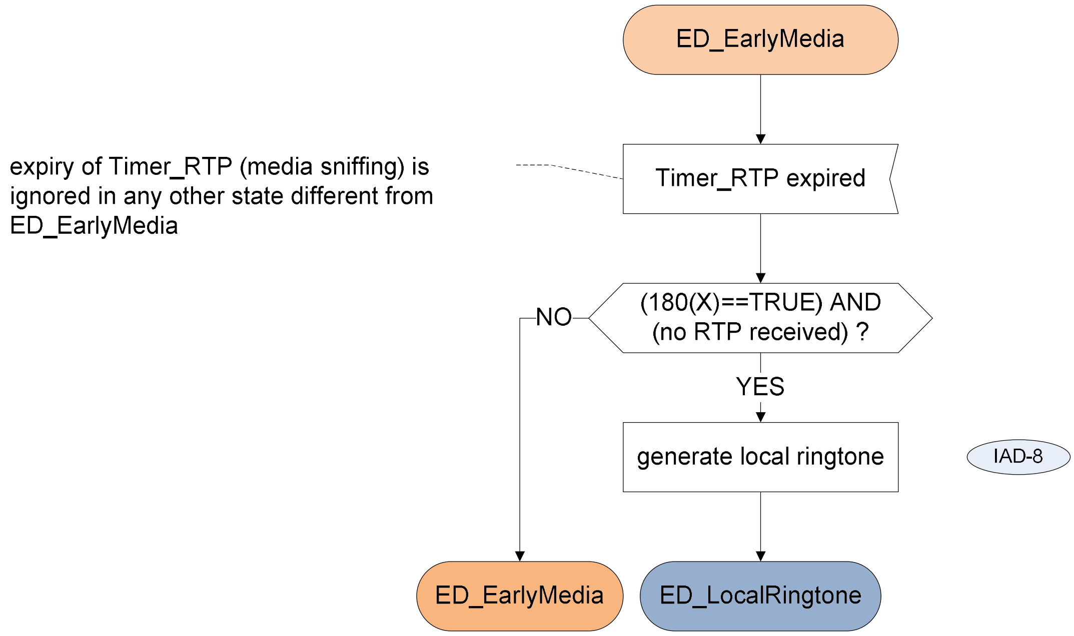


Figure G.2.4.1: Timer Check during state ED_EarlyMedia

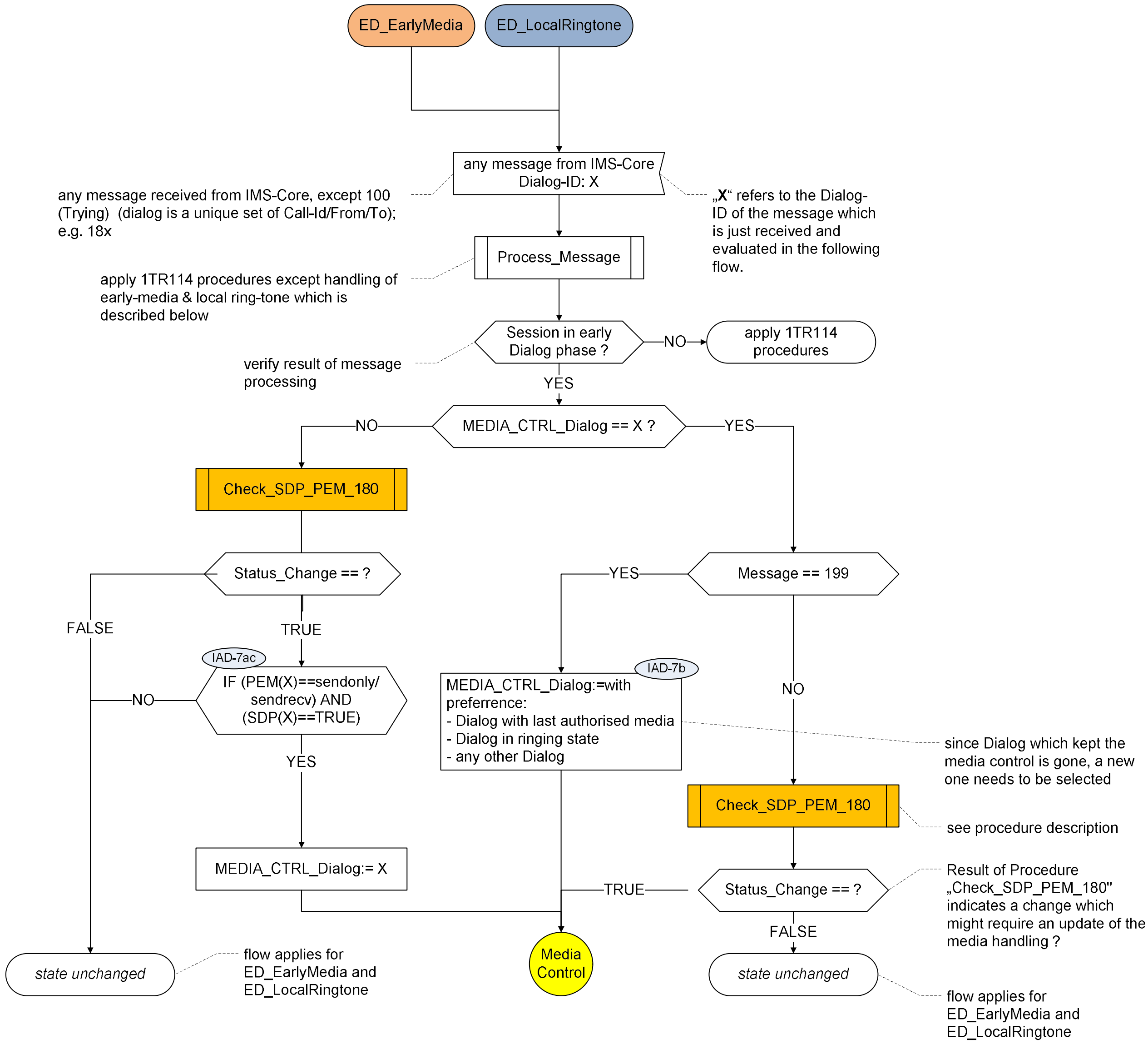
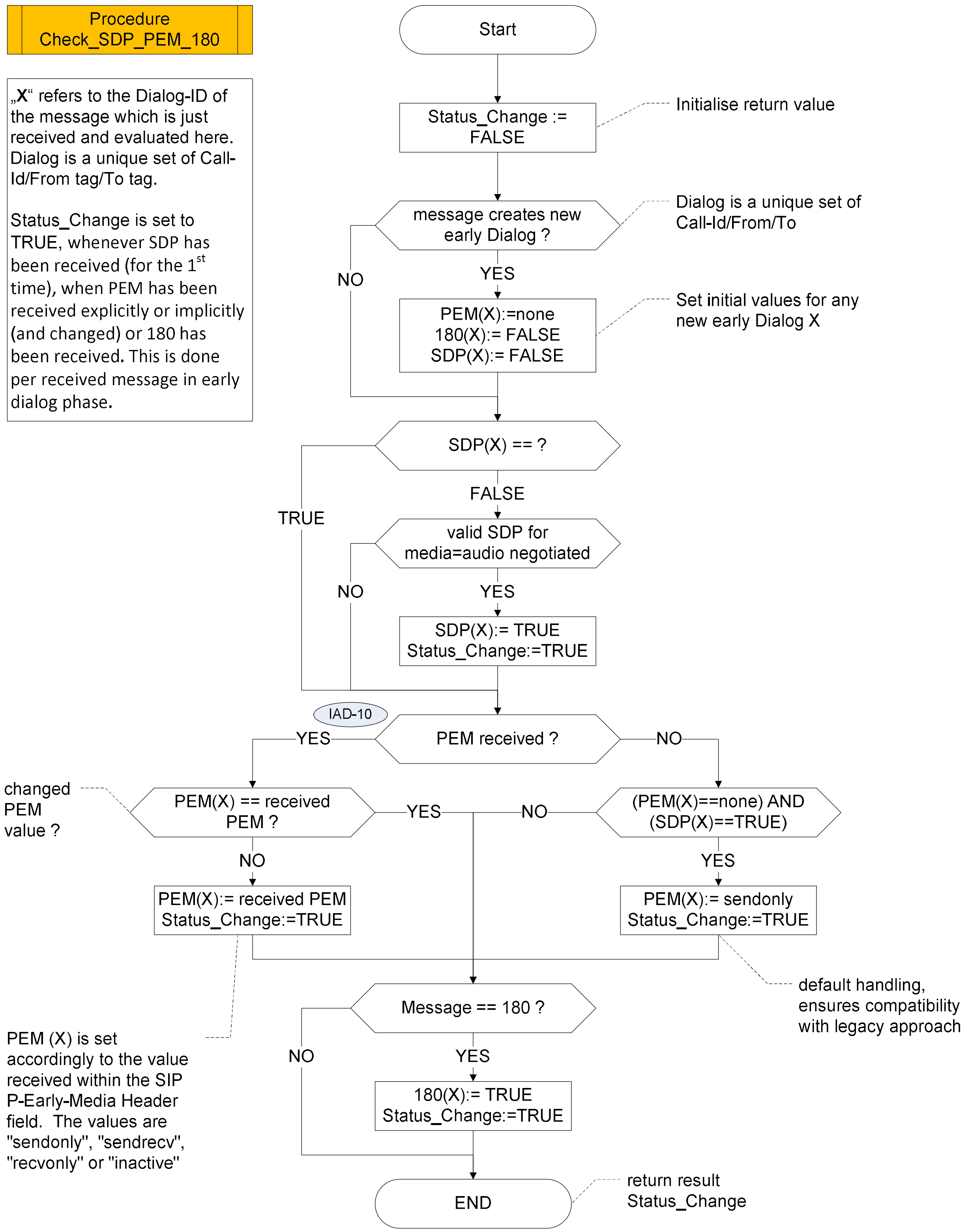


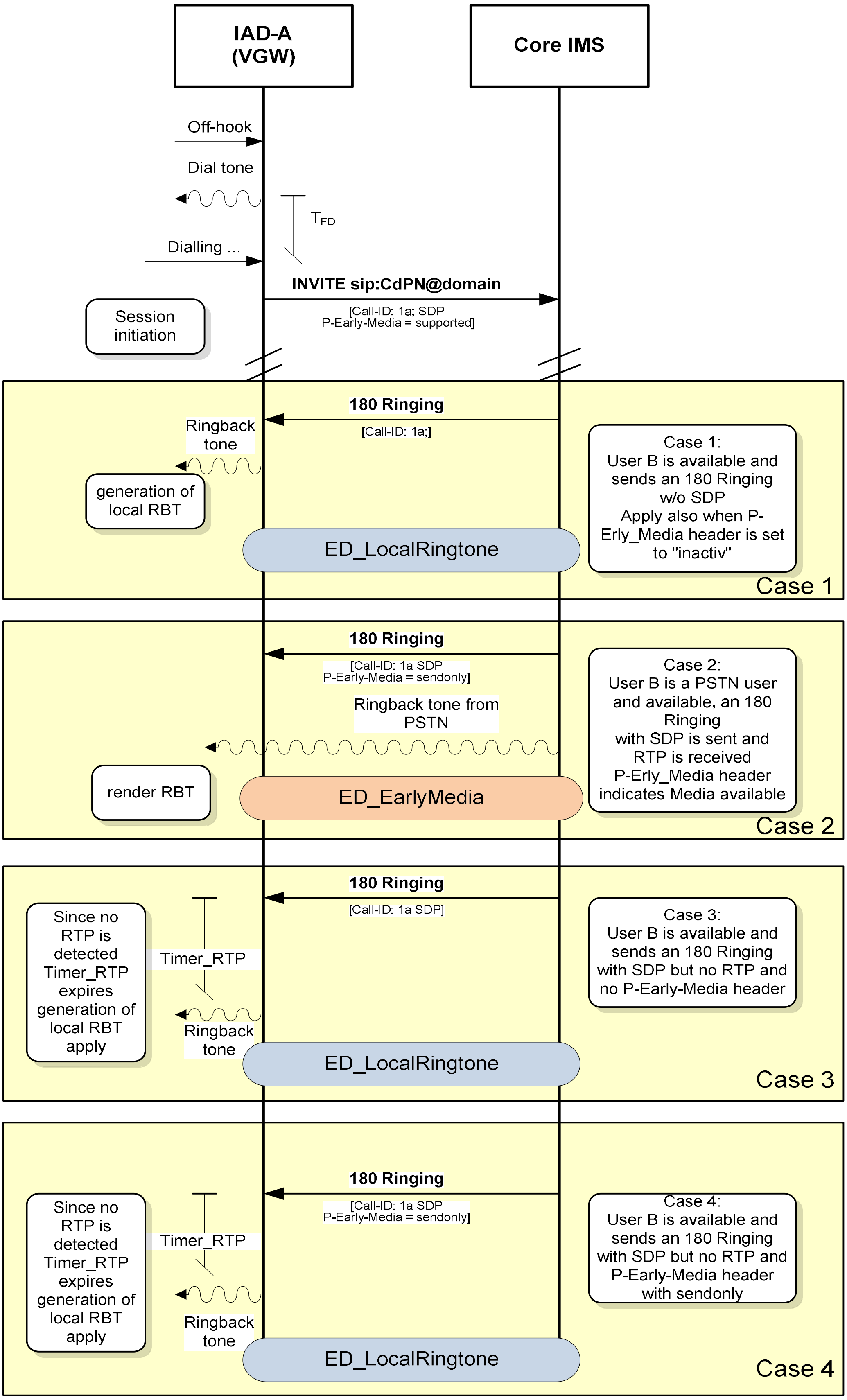
Figure G.2.4.2: State EarlyDialog_EarlyMedia & State EarlyDialog_LocalRingtone

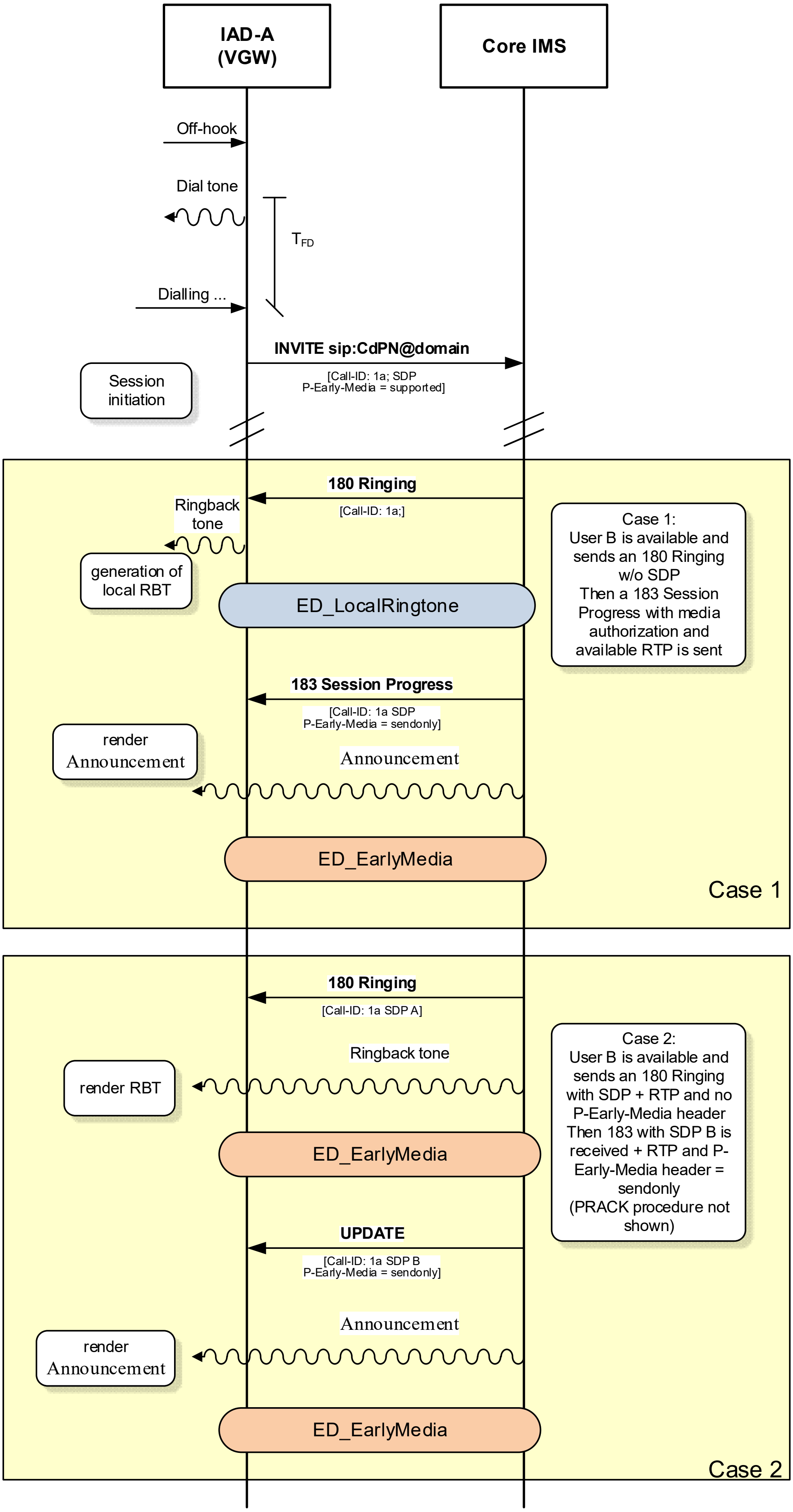
G.2.4 Procedure Check_SDP_P-EARLY-MEDIA_180

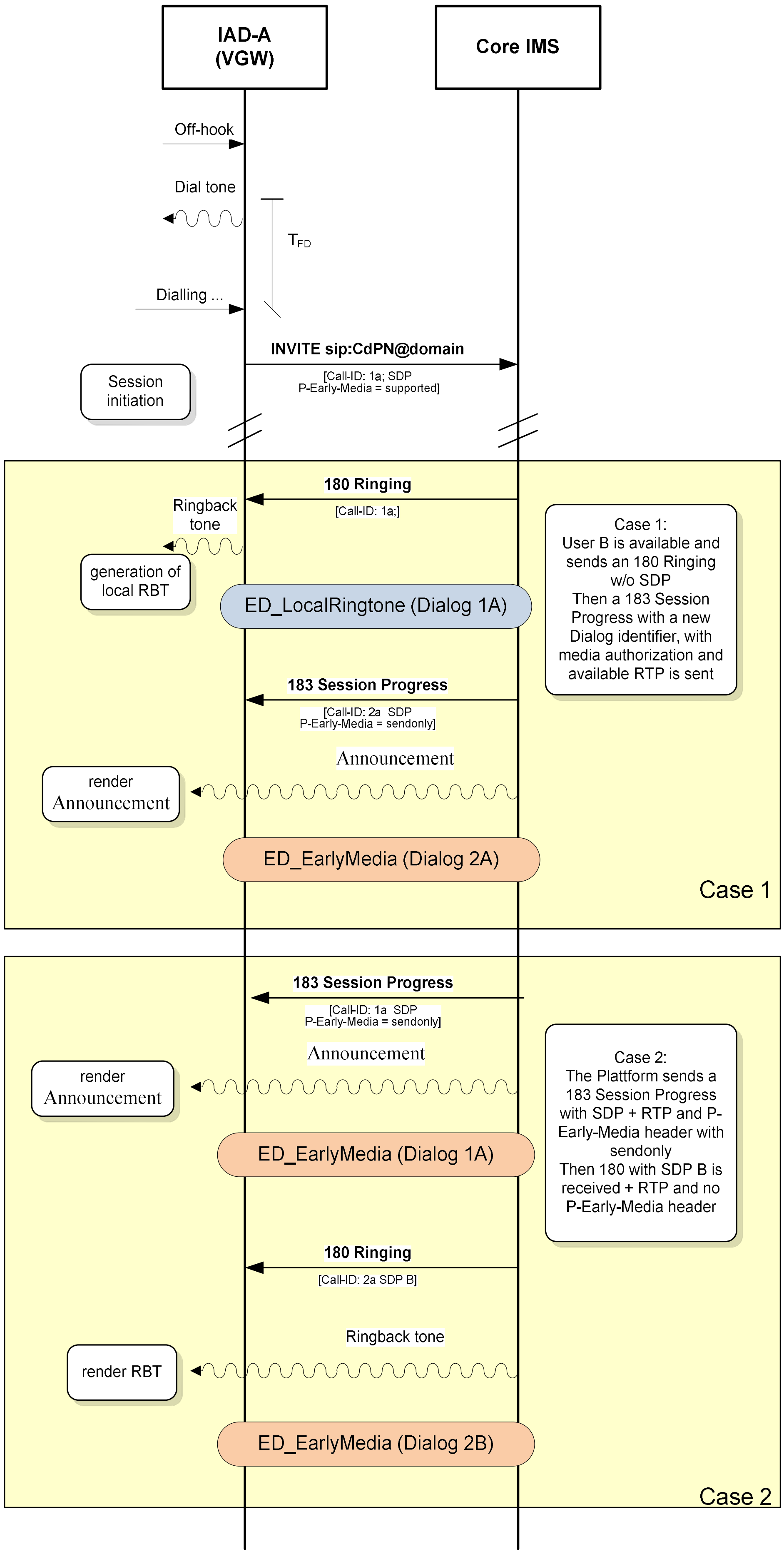


FigureG.2.5.1: Procedure Check_SDP_P-EARLY-MEDIA_180

ANNEX H (informative) Call Flows Early Media


IAD-A (VGW)
Core IMS
Off-hook
Dial tone
TFD
Dialling ...
INVITE sip:CdPN@domain
[Call-ID: 1a; SDP
P-Early-Media = supported]
Session initiation
180 Ringing
[Call-ID: 1a;]
Ringback tone
generation of local RBT
ED_LocalRingtone
Case 1:
User B is available and sends an 180 Ringing w/o SDP
Apply also when P-Erly_Media header is set to "inactiv"
Case 1
180 Ringing
[Call-ID: 1a SDP
P-Early-Media = sendonly]
Ringback tone from PSTN
render RBT
ED_EarlyMedia
Case 2:
User B is a PSTN user and available, an 180 Ringing
with SDP is sent and RTP is received
P-Erly_Media header indicates Media available
Case 2
180 Ringing
[Call-ID: 1a SDP]
Since no RTP is detected Timer_RTP expires generation of local RBT apply
Timer_RTP
Ringback tone
ED_LocalRingtone
Case 3:
User B is available and sends an 180 Ringing with SDP but no RTP and no P-Early-Media header
Case 3
180 Ringing
[Call-ID: 1a SDP
P-Early-Media = sendonly]
Since no RTP is detected Timer_RTP expires generation of local RBT apply
Timer_RTP
Ringback tone
ED_LocalRingtone
Case 4:
User B is available and sends an 180 Ringing with SDP but no RTP and P-Early-Media header with sendonly
Case 4

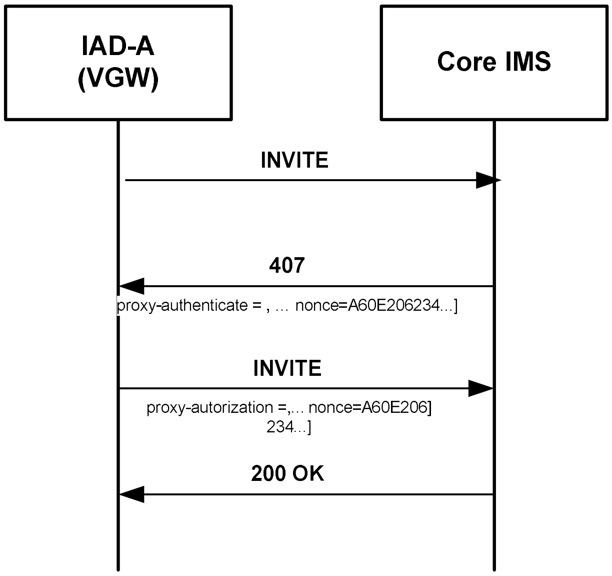

IAD-A (VGW)
Core IMS
Off-hook
Dial tone
T_FD
Dialling ...
INVITE sip:CdPN@domain
[Call-ID: 1a; SDP
P-Early-Media = supported]
Session initiation
180 Ringing
[Call-ID: 1a;]
Ringback tone
generation of local RBT
ED_LocalRingtone
Case 1:
User B is available and sends an 180 Ringing w/o SDP
Then a 183 Session Progress with media authorization and available RTP is sent
183 Session Progress
[Call-ID: 1a SDP
P-Early-Media = sendonly]
render Announcement
Announcement
ED_EarlyMedia
Case 1
180 Ringing
[Call-ID: 1a SDP A]
Ringback tone
render RBT
Case 2:
User B is available and sends an 180 Ringing with SDP + RTP and no P-Early-Media header
Then 183 with SDP B is received + RTP and P-Early-Media header = sendonly
(PRACK procedure not shown)
ED_EarlyMedia
UPDATE
[Call-ID: 1a SDP B
P-Early-Media = sendonly]
Announcement
render Announcement
ED_EarlyMedia
Case 2


IAD-A
(VGW)
Core IMS
Off-hook
Dial tone
TFD
Dialling ...
INVITE sip:CdPN@domain
[Call-ID: 1a; SDP
P-Early-Media = supported]
Session initiation
180 Ringing
[Call-ID: 1a;]
Ringback tone
generation of local RBT
ED_LocalRingtone (Dialog 1A)
Case 1:
User B is available and sends an 180 Ringing w/o SDP
Then a 183 Session Progress with a new Dialog identifier, with media authorization and available RTP is sent
183 Session Progress
[Call-ID: 2a SDP
P-Early-Media = sendonly]
Announcement
render Announcement
ED_EarlyMedia (Dialog 2A)
Case 1
183 Session Progress
[Call-ID: 1a SDP
P-Early-Media = sendonly]
Announcement
render Announcement
Case 2:
The Plattform sends a 183 Session Progress with SDP + RTP and P-Early-Media header with sendonly
Then 180 with SDP B is received + RTP and no P-Early-Media header
ED_EarlyMedia (Dialog 1A)
180 Ringing
[Call-ID: 2a SDP B]
Ringback tone
render RBT
ED_EarlyMedia (Dialog 2B)
Case 2

Annex I Examples for Challenge

I.1. Challenge when INVITE does not contain Proxy-Authorization header

Initial Request does not contain any authorization header, thus a challenge is needed to reflect the validity of the registering UE (IAD)



<u>Initial Request INVITE w/o Authorization header</u>

<u>Challenge Request in SIP Response 407:</u>

Proxy-Authenticate

Digest nonce="A60E206B33C999900000000DAA2F522"

,realm="tel.t-online.de",

algorithm=MD5,

qop="auth"

<u>Answer in following INVITE:</u>

Proxy-Authorization:

username="Alice@t-online.de",

realm="tel.t-online.de",

Digest nonce="A60E206B33C999900000000DAA2F522",

uri="sip:+Alice_E164@tel.t-online.de",

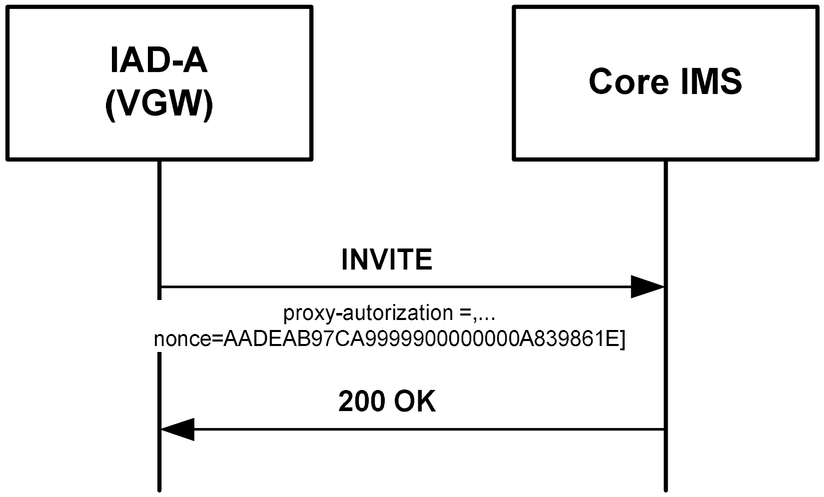
response="3d0ae894faee9999d0cfe7fcce5ee402", algorithm=MD5,

cnonce="E013376E7888856D",

qop=auth,

nc=00000001

I.2 Example with correct Proxy-Authorization header in INVITE



Exampe initial INVITE using nonce from Registration:

Proxy-Authorization:

Digest username="Alice@t-online.de",

realm="tel.t-online.de",

nonce="AADEAB97CA9999900000000A839861E",

uri="sip:Alice_E164@tel.t-online.de;

user=phone;transport=udp",

response="e7c5f54f744dd8f88b63e84052

Algorithm: MD5

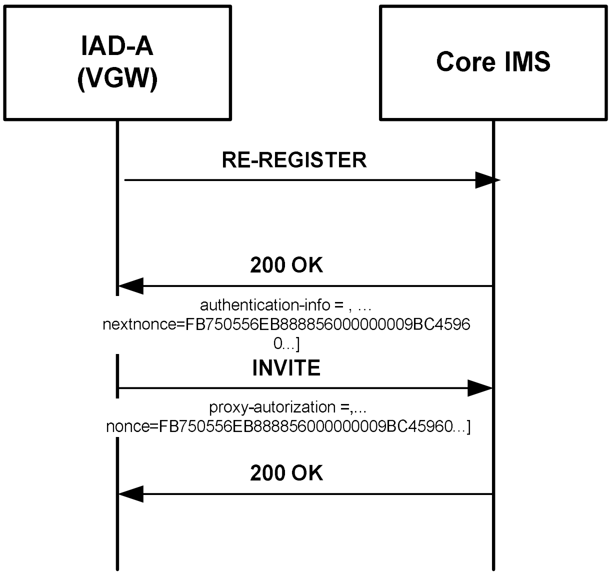
CNonce Value: "568a61bf"

QOP: auth

Nonce Count: 00001234

The nonce value was exchanged during registration procedure and stored within the IAD.

I.3 Example with correct Authentication-Info header in 200 OK for REGISTER



200OK for Re-Register

Authentication-Info:

nextnonce="FB750556EB888856000000009BC45960",

qop=auth,

rspauth="b385ad644ba1f25cc32e2dbbf3cc166c",

cnonce="568a61cc",

nc=00001234

Example initial INVITE using nonce from 200 OK (REGISTER):

Proxy-Authorization:

Digest username="Alice@t-online.de",

realm="tel.t-online.de",

nonce=" FB750556EB888856000000009BC45960",

uri="sip:Alice_E164@tel.t-online.de;

user=phone;transport=udp",

response="e7c5f54f744dd8f88b63e84052

Algorithm: MD5

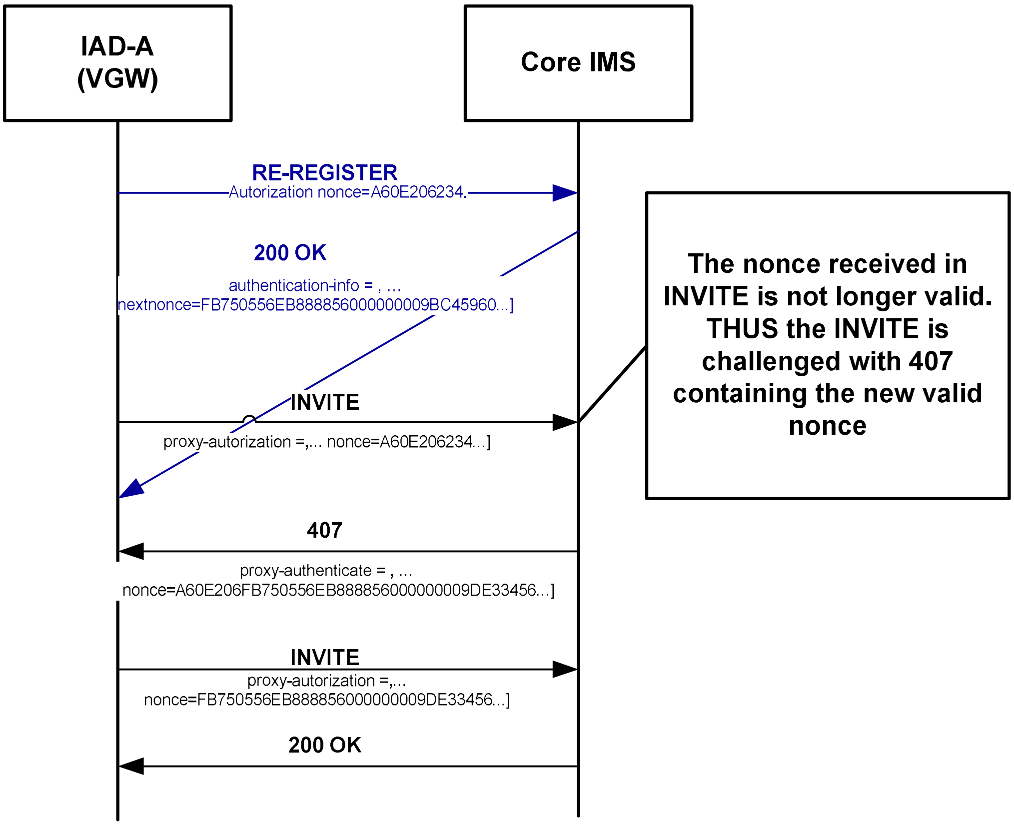
CNonce Value: "568a61bf"

QOP: auth

Nonce Count: 00001234

Note: Authentication-Info is currently not used for 200 OK answering an INVITE request.

I.4 Example with race condition Authentication-Info header in 200 OK for REGISTER crosses INVITE with "old nonce"



ANNEX J (informative) Implementation of VoSIP using mediasec extension

This Annex shows some call flows for providing more information due to the implementation of the mediasec parameter to be compliant with the Deutsche Telekom Gm interface.

The mediasec parameter orientate on draft-dawes-dispatch-mediasec-parameter-08.txt [79] which is an enhancement of RFC 3329.

```
6.1     Initial Registration and Invite

  At initial registration, the client includes its supported media
  plane security mechanisms in the SIP REGISTER request. The registrar
  return its supported media plane security mechanisms in the
  SIP 401 (Unauthorized) response.

  A client is still required to ask for verification of all
  supported security mechanisms even if only sdes-srtp; mediasec is
  technically supported, as shown in Figure 1 below.
```

```
Within initial Invite the client includes the registrar supported media
plane security mechanisms from the SIP 401 (Unauthorized) response. In
SDP the attribute "a=3ge2ae:requested" is required for indication of end
to access edge media security. The registrar supported media plane
security mechanisms need to be added from client for verification also
to Re-Invite or Update messages.


UAC                         Registrar
|                           |
|----(1) REGISTER------------------------------->|
|    Security-Client: sdes-srtp;mediasec  |
|    Proxy-Require: mediasec        |
|    Require: mediasec           |
|                           |
|<---(2) 401-------------------------------------|
|    Security-Server: msrp-tls;mediasec   |
|    Security-Server: sdes-srtp;mediasec  |
|    Security-Server: dtls-srtp;mediasec  |
|                           |
|----(3) REGISTER(with Authorization Header)--->|
|    Security-Client: sdes-srtp;mediasec  |
|    Proxy-Require: mediasec        |
|    Require: mediasec           |
|    Security-Verify: msrp-tls;mediasec   |
|    Security-Verify: sdes-srtp;mediasec  |
|    Security-Verify: dtls-srtp;mediasec  |
|                           |
|<---(4) 200 OK---------------------------------|
|                           |
|                           |
|----(5) INVITE--------------------------------->|
|    Security-Verify: msrp-tls;mediasec   |
|    Security-Verify: sdes-srtp;mediasec  |
|    Security-Verify: dtls-srtp;mediasec  |
|    a=3ge2ae:requested          |
|    a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:EpcgtOdT5qd...
|                           |
|<---(8) 200 OK---------------------------------|
|    a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:lnfakjh2sd1...

  Figure 1: Exchange of Media Security Mechanisms at Initial
            Registration and Invite
```

ANNEX K (informative) guideline which section is valid for 1TR118/1TR119

The following sections do not apply for business end devices in combination with 1TR118[91]/1TR119 [92]:

Annex D

ANNEX L Void

ANNEX M Abbreviations

Abbreviations, definitions and symbols not listed hereafter, are defined in the reference documents in clause 2.

Annex M1 Abbreviations

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

-1-

3DES	Triple DES
3GPP	Third Generation Partnership Project
3GPP TS	3GPP Technical Specification (normative)
3PCC	Three Party Call Control
3PTY	Three party conference

-A-

AAA	Authorization Authentication Accounting
ACR	Anonymous Communication Rejection
ack.	Acknowledge (tone or announcement)
AES	Advanced Encryption Standard
AS	Application Server

-B-

-C-

CC	Call Control
CC	Country Code
CCBS	Completion of Communications to Busy Subscriber
CD	Communication session Deflection
CDIV	Communication Diversion Services
CFB	Communication session Forwarding Busy
CFN	Call Forwarding Number, e.g. <CFN>
CFNR	Communication session Forwarding No Reply
CFU	Communication session Forwarding Unconditional
CLID	Calling Line Identification
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction

CN	Calling Number (Calling Party Number), e.g. <CN>
COLP	Connected Line Identification Presentation
COLR	Connected Line Identification Restriction
CONF	Conference (Konferenz)
CW	Call Waiting
-D-	
DDI	Direct Dial In
DIPVD	DeutschlandLAN IP Voice/Data
DIV	Digitales Vermittlungssystem
DH	Diffie–Hellman
DHE	Diffie–Hellman Ephemeral
DN	Destination Number, e.g. <DN>
DNS	Domain Name System
DSA	Digital Signature Algorithm
DSLAM	Digital Subscriber Line Access Multiplexer
DSS	Digital Signature Standard
DT	Deutsche Telekom
-E-	
ECDH	Elliptic curve Diffie–Hellman
ECDHE	Elliptic curve Diffie–Hellman ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
ES	European Standard
ETSI	European Telecommunication Standardisation Institute
ETSI ES	ETSI Standard (normative)
ETSI TR	ETSI Technical Report (informative)
ETSI TS	ETSI Technical Specification (normative)
ETSI/TISPAN	Merger of ETSI Project Tiphon and ETSI Technical Body SPAN
EVS	Enhanced Voice Services
-F-	
FCR	Forwarded Communication Restriction
-G-	
G-ISUP	Gateway ISUP

GRUU	Globally Routable User Agent URI
-H-	
HMAC	Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
-I-	
IAD	Integrated Access Device
IAF	Internet-aware fax device
IARI	IMS Application Reference Identifier
ICSI	IMS Communication Service Identifier
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
INTIME	Independent Timer
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IMPU	IMS Public Identity
ISDN	Integrated Services Digital Network
ISIM	IM Subscriber Identity Module
ISUP	ISDN User Part
ITU-T	International Telecommunication Union, Telecommunication Branch
IWU	Interworking Unit
-J-	
-K-	
-L-	
-M-	
MCID	Malicious Call Identification
MEGACO	Media Gateway Control Protocol
MG	Media Gateway
MGC	Media Gateway Controller
MIME	Multipurpose Internet Mail Extensions
MMS	Multimedia Message Service
MSN	Multiple Subscriber Number

MTP	Message Transfer Part
MWI	Message Waiting Indicator
-N-	
NAPT	Network Address Port Translation
NAS	Network Access Server
NASS	Network Attachment Subsystem
NAT	Network Address Translation
IMS	Next Generation Networks
-O-	
OIP	Originating Identification Presentation
OIR	Originating Identification Restriction
ON	Originating Number, e.g. <ON>
-P-	
PCM	Pulse Code Modulation
PDU	Protocol Data Unit
PIN	Personal Identification Number
PINnew	new PIN (4 digits)
PINold	old PIN (4 digits)
PPP	Point to Point Protocol
PPPoE	Point to Point Protocol over Ethernet
PSTN	Public Switched Telephone Network
PUID	Public User Identity
-Q-	
QoS	Quality of Service
-R-	
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments
RSA	Rivest, Shamir und Adleman
RTCP	Real Time Control Protocol
RTP	Real Time Transport Protocol
-S-	
SCC	Service Code Command
SCTP	Stream Control Transmission Protocol

SDES	Source Description RTCP Packets
SDP	Session Description Protocol
SHS	Secure Hash Standard
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SIP I	SIP ISUP (SIP with encapsulated ISUP MIME)
SIP T	SIP Telephony
SMS	Short Message Service
SN	Subscriber Number
SOC	Switching Order Command
SS	Supplementary Service
STUN	Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs); also: Session Traversal Utilities for NAT
-T-	
TAS	Telephony Application Service
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TDM	Time Division Multiplex
TIP	Terminating Identification Presentation
TIR	Terminating Identification Presentation Restriction
T-ISUP	Telekom ISUP
TLS	
TR	Technical Recommendation
TR	Technical Report [ETSI]
TS	Technical Specification
TS	Technical Specification [ETSI]
-U-	Transport Layer Security
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	User Datagram Protocol
UE	User Equipment
UICC	Universal Integrated Circuit Card

UNI	User Network Interface
URI	Universal Resource Identifier
URL	Uniform Resource Locator
-V-	
-W-	
-X-	
xDSL	x Digital Subscriber Line (x stands for various kinds of bit rates)
XML	Extended Markup Language
-Y-	
-Z-	

History

Version	Published	Remarks
1.0	15.05.2009	First edition of 1 TR 114
1.1	05.11.2009	Updated edition of 1 TR 114 Version 1.0: - General formal changes (editorial); - Foreword updated; - References updated (RFC 2411, RFC 4734 and RFC 5244 added, RFC 2833 deleted); - 3.1 Abbreviations updated; - 3.3 Symbols updated; - Clause 4.2.1 (A-law and µ-law added, DTMF moved to 4.2.4); - Clause 4.2.4 added (DTMF); - Clause 6: Note added; - Clause 7.1.1 updated (also: “TLS is not used” deleted, global number format, challenge mechanism, DNS SRV); - Clause 7.2 updated: §5.1.1.2A added and modified, §5.1.2A.1: P-Preferred-ID, §9.2.1: DNS procedures added, §9.2.1 added and modified, Table A.4 modified (Item: 89, DT1; Condition: c17, c90, c_dt4); - Clause 7.3 updated: Table 7-1 modified; - Clause 7.3.2 updated: Table 7-2 (item numbering and conditions modified; Overlap deleted); - Clause 7.3.3 updated: Table 7-3 (item: 101A added) - Clause 7.3.4 updated: Table 7-4 (item 33b and 36a added, 39, 61b and 70a modified, conditions c6, c7, c9 and Note 4 modified); - Clause 7.3.5 updated: Table 7-5 (condition c1 modified); - Clause 7.3.6 “SDP Types” (new): §A3.2.2 added; - Clause 7.4.1 updated: Table 7-6 (Ref. modified and column “Support” added, IPSec added); - Clause 7.4.2: Table 7-7, Table 7-8 and Table 7-9 updated; - Clause 7.4.3: Table 7-10 updated; - Clause 7.4.4 (new) “Real time Transport Procedures” added: Table 7-11 added; - Clause 8.4 (new) “Network access” added; - Clause 8.5 (new) “Number handling by the UE” added; - Clause 8.6 (new) added: “Support of NAT traversal by the UE”; - A.2.1.1: Footnote 1 added; - A.2.2: Note and footnote added; - A.2.4 (§4.5.2.1): modified (anonymous and display name not allowed); - A.2.6: modified (re-INVITE); - B.2: Updated (CLIR 3 becomes CLIR/OIR) and Note added; - B.8: Updated and footnote added; - B.10: Updated and footnote added; - B.11: Footnote added; - B.13: Updated and footnote added; - B.15: Updated and footnote added;

Version	Published	Remarks
		- B.19: Procedures “336” changed to “339”; - B.20 (B.20.1.2): corrected; - B.21 (B.21.1.2): corrected; - B.23 (B.23.1.2): corrected; - B.24 (B.24.1.2 and B.24.1.4): corrected; - B.25 (B.25.1.2): corrected; - B.26 (B.26.1.1 and B.26.1.2): corrected; - B.27 (B.27.1.1): corrected; - B.28 (ECT) completed (added); - Annex C (Supervisory tones) added.
2.0	30.06.2010	Second edition of 1 TR 114: - General (formal) updates; - Foreword corrected; - Endorsements of ETSI TS124 503 and 3GPP TS 24.229 (modifications) moved to Annex A and Annex B; - Endorsement part (new Annex A and new Annex B) deleted and general text updated; - References updated and V.152 and T.30 added; - Reference [36] added; - Reference to µ-Law deleted in clauses 4.2.2 and 6. (Table 6-1); - Clause 4.2.1 (new): SIP capabilities inserted; - Clause 4.2.3 Fax and Modem: Text modified (T.38 not supported) - Clause 5.2: DDI text deleted; - Clause 7.1.1 : Text (HEX digits) added; - Clause 7.1.1 and C.2.11.1: bidirectional early media clarified; - Clause 7.3.4 (Table 7-4): c5 “(REFER)” added; - Clause 7.4.2: condition c1 deleted and RFC 4443 set to “m”; - Clause 7.4.4: RFC 4040 added; - Clause 7.4.4: NOTE2 added; - Clause 8.4.1: G.711a explicit specified; - Table 7-2: Supported methods (Item 12: “o” changed to “m” and Note 1 added); - Table 7-3 : note 5 added; - Table 7-7: reference to RFC 0792 added; - Table headers corrected; - Priority of Annex A against Annex B clarified; - Annex B: already deleted clause 5.1.1.2.1 reactivated, again; - Clause C.2.10 (§4.5.2.1): bullet point added (Session-ID); - Clause C.2.12: Text (AOC) added; - Clauses C.2.12.1 … C.2.12.3 updated; - Delta list in History added (for V1.1); - T-Home replaced by Deutsche Telekom; - Zentrum Technik Einführung (ZTE) replaced by Fixed Mobile Engineering Deutschland (FMEd); - Document properties updated; - History updated.
2.1	22.07.2010	Updated edition of 1 TR 114 (V2.0): - Formal corrections; - Clause 3.1: Updated; - Clause 7.4.4: Requirement for RTCP/SDES added; - Clause 7.1.1: Support of GRUU (mandatory) and Instance-ID

Version	Published	Remarks
		added; - Annex C.1: First sentence corrected (GRUU is used); - References RFC 4122 and RFC 5626 added; - Annex C.2.6: Text added (bandwidth); - References RFC 3890 added; - References RFC 5627 added; - Clause 7.1.1: Bullet point concerning Call-Id added; - Annex D: Editorial changes; - Annex D.7: Prerequisite for 3PTY added; - Annex D.8.1.3, D.9.1.3 and D.10.1.3: Footnote added; - Annex D.11.1.3, D.12.1.3 and D.13.1.3: Footnote added; - Annex D.14.1.3 and D.14.1.4 swapped; - Annex D.14.1.3, D.15.1.3: Footnote added. - Endorsement References of ETSI TS124 503 and 3GPP TS 24.229 modified to 1TR114 Annex A Version 1.1.0 and 1TR114 Annex B Version 1.1.0;
2.2	18.02.2011	- Formal changes (Version number on cover page); - Reference to ETSI TS 124 505 deleted; - Reference to ETSI TS 124 605 (Release 9) added; - Annex C.2.2: Reference updated; - Table Annex E 1: State P4 deleted and “off-hook state” added; ; - Clause §4.5.2.1: “may” replaced by “shall; - Annex C.2.8 CW: Note added (ghost ringing); ; - Annex C.2.10 ECT: Paragraph §A.2 and note added (call flow); ; - Fetch Binding Requests shall not apply or shall be used minimal.
2.2.1	01.03.2011	- Editorial Change of Date - Note added for DTMF use when not supporting RFC4733
2.3.0	13.04.2011	- Editorial: reinstallation of correct numbering - Marking of features which will be not supported in September 2011 - Reference RFC4884 added. Section 1, Table 7.-7 (needed for IPv6), - IPv6 Procedures added Section 8.2 and 8.3 - Addition of clarification for implicit registration procedure for implicit registration sets in HSS (use of P-Associated-URI header) Section 7.7.1 - Activation option via TR-069 [72], TR-181 [74] AND TR104 [72] for HOLD, CW, TOGGEL and CONF added, Section 5.1 and ANNEX C - Configuration option for local CW Section 5.1 - implicit registration for "ua-profile" included, Section 4.2.1 - Table 7-2 PUBLISH behaviour corrected - Table 7-2 REGISTER behaviour corrected - Table 7-2 UPDATE behaviour corrected
2.4.0	15.12.2011	Main Change is that the procedures for CONF/3PTY, HOLD, CW and TOGGLE where changed from a centric network approach to the implementation within the end device. Foreword, better description to understand the structure of the document (editorial) Section 4.2.1 editorial write up to understand requirements on

Version	Published	Remarks
		preconditions. (editorial) Section 7.1.1 editorial extensions for better understanding, Section7.1.1 deletion of GRUU, Section 7.1.1 Addition of early Challenge procedure Section 7.1.1 Addition of REGISTER procedure in case of the receipt of 403 Page 40, Note5 geändert um weitere Registrierung mit gleichem Contact zuzulassen auch bei 403. Table 7-4 Refer-sub added, Prox-Authentication entry corrected. (editorial) Table 7-3 new Status Code ended 469 (Bad INFO Package) (editorial/default behaviour) 7.4.1 Note in Table 7-6 shifted. (editorial) C.2.2 (CONF) corrected for VGW internal Service execution C.2.6 (HOLD) corrected for VGW internal Service execution C.2.8 (CW) corrected for VGW internal Service execution D.5 (CW) Addition of general procedure for VGW internal Service execution D.6 (HOLD/TOGGLE) Addition of general procedure for VGW internal Service execution D.7 (CONF) Addition of general procedure for VGW internal Service execution Comment included on Option for Implementing *# and SIP Procedures.
3.0.0		-locating P-CSCF and correct prioritization of P-CSCF in case of registration including maintenance procedures. -Preconditions support "passive" better described -Early-Media Header and indication of early media described to avoid misinterpretation. And allow handling of calls initiated by mobile devices. - use of from-change. No default setting - deletion of Annex A - Update of Annex B - Deletion of TS 124.503 - UPDATE to 3GPP Release 11 documents -Correction of *# Procedures using PIN (ECT, OCB, Kick Out, Black List, White List, ACR, CB, ICB) - CLIR 3 included in D.2.0 - Documentation Update TIP/TIR and OIP/OIR -MWI voided - Documentation Update of " 8.6 Support of NAT traversal by the UE" -MIME Type UPDATE Table 7-5 -UPDATE Table 7-4 SIP Headers - add references TR-069, TR-104 and TR-181 - add reference 3GPP TS 23.003 - C.2.8 allow implementations acting on "application/vnd.3gpp.cw+xml" All changes are backward compatible with the procedures described within 1TR114 Version 2.4.0
4.0.0	07.01.2019	Implementation of all Amendments and complete editorial rework of document.

Version	Published	Remarks
		Rewriting of VoSIP using mediasec extension for a better reflection of DT network behaviour. Addition of examples and clarifications.
4.1.0	December 2019	Editorial Changes (references & numbering) Only T.38 over UDPTL shall be supported Support of AMR and EVS is changed
4.2.0	March 2022	Sending of STUN for pin holing disabled a-records request only is NOT allowed Correction of informative VOSIP Call flow for implementation. New SOC for Time depended CDIV Aktivierung: *621# Aktivierung mit Ziel: *621*<target># Deaktivierung: #621# INVITE without SDP Hint for RFC3605 Reaction when DSN Request fails Use of visual separators Rules for number block +49116XXX Preconditions are not supported in DT IMS fixed network Note on 2nd offer in early dialog phase Cipher List: double entries voided Clarification on DTMF TLS 1.3 added TLS 1.1 no longer allowed Update according to BSI 02102-2 (2021) Deletion of ECT which is no longer a consumer service Message size 8kB Deletion of DHE Cipher suites due to security constrains
4.3.0	March 2024	Procedures included for TCP non-reachability