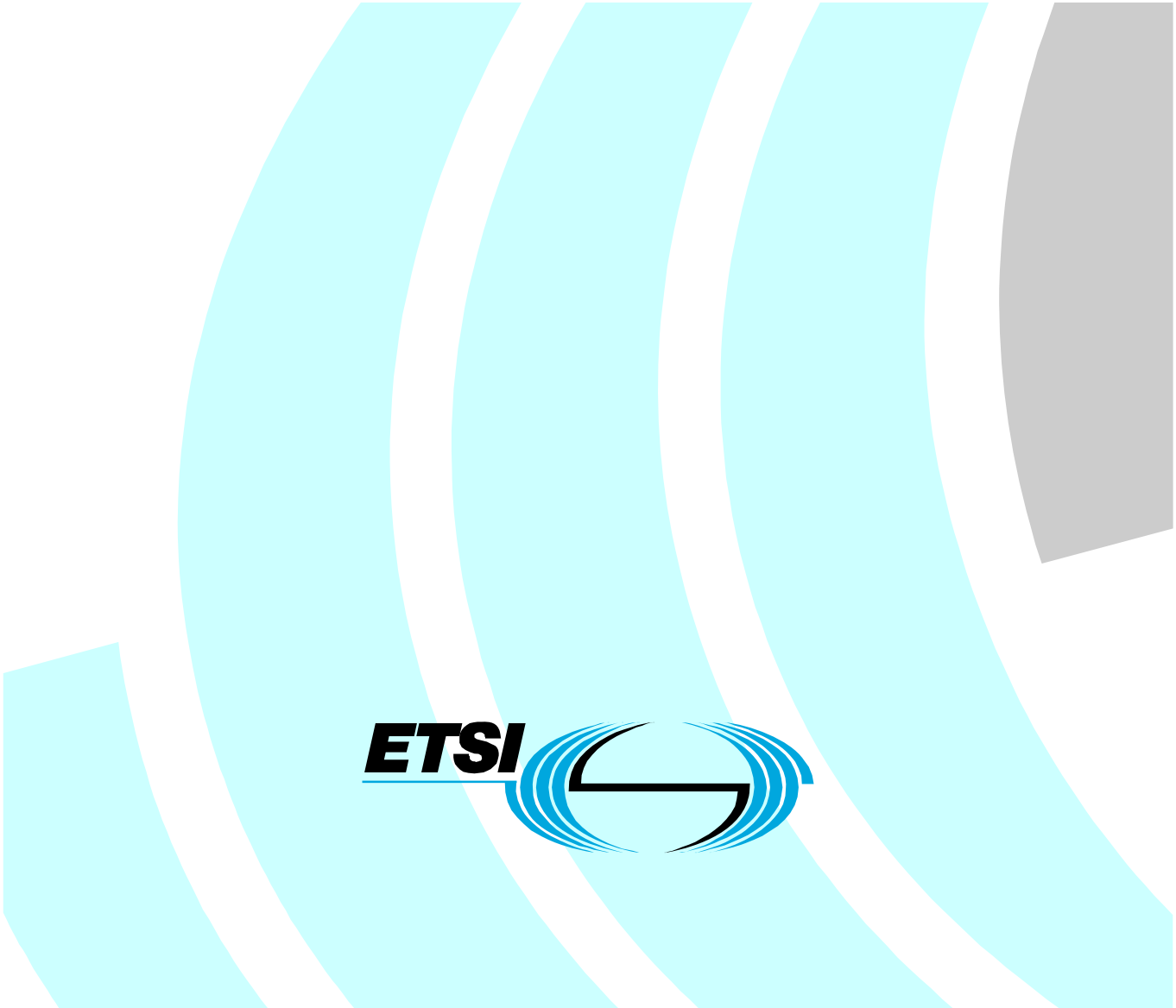
ETSI TS 185 010 V2.1.1 (2009-07)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Premises Networks: Protocol Specification (Stage 3)



Reference
DTS/TISPAN-05019-NGN-R2

Keywords
protocol

ETSI

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

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

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

Contents

Intellectual Property Rights

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

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

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document describes the protocols used for the reference points internal to the Customer Premises Network (CPN), between the Customer Network Gateway (CNG) and the Customer Network Devices (CNDs). This description is based on the architecture and stage 2 information flows contained in TS 185 003 [1] and TS 185 006 [2].

The reference points between the IPTV CND [3] and the CNG are not covered by the present document. These reference points are detailed in TS 185 011 [12].

2 References

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.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

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

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

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ETSI TS 185 003 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Network Gateway Architecture and Reference Points".

NOTE: The latest version in the V2.y.z series applies.

[2] ETSI TS 185 006 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Devices architecture and Reference Points".

NOTE: The latest version in the V2.y.z series applies.

[3] draft-saito-mmusic-sdp-ike-03 (July 27 2008): "Media Description for IKE in the Session Description Protocol (SDP)".

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

[5] ETSI ES 283 003 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 [3GPP TS 24.229 [Release 7], modified]".

NOTE: The latest version in the V2.y.z series applies.

[6] UPnP™: "UPnP™ Device Architecture 1.0 (24 April 2008)".

NOTE: Available at http://www.upnp.org/specs/arch/UPnP-arch-DeviceArchitecture-v1.0.pdf.

[7] UPnP™: "MediaServer:3 Device Template Version 1.01 (30 September 2008)".

NOTE: Available at http://www.upnp.org/specs/av/UPnP-av-MediaServer-v3-Device.pdf.

[8] ETSI TS 124 504 (V8.4.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); TISPAN; PSTN/ISDN simulation services: Communication Diversion (CDIV); Protocol specification (3GPP TS 24.504 version 8.4.0 Release 8)".

[9] ETSI TS 124 411 (V8.1.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); TISPAN; PSTN/ISDN simulation services: Anonymous Communication Rejection (ACR) and Communication Barring (CB); Protocol specification (3GPP TS 24.411 version 8.1.0 Release 8)".

[10] ETSI TS 124 529 (V8.0.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); TISPAN; PSTN/ISDN simulation services: Explicit Communication Transfer (ECT); Protocol specification (3GPP TS 24.529 version 8.0.0 Release 8)".

[11] ETSI TS 124 410 (V8.0.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); TISPAN; NGN Signalling Control Protocol; Communication HOLD (HOLD) PSTN/ISDN simulation services; Protocol specification (3GPP TS 24.410 version 8.0.0 Release 8)".

[12] ETSI TS 185 011 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Specification of Protocols for Customer Network Devices enabling the IMS-based IPTV service usage".

NOTE: The latest version in the V2.y.z series applies.

[13] ETSI TS 124 406 (V8.0.0) : "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); TISPAN; PSTN/ISDN simulation services; Message Waiting Indication (MWI): Protocol specification (3GPP TS 24.406 version 8.0.0 Release 8)".

[14] IETF RFC 4572: "Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)".

[15] ETSI TS 183 006 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Message Waiting Indication (MWI): Protocol specification".

NOTE: The latest version in the V2.y.z series applies.

[16] ETSI ES 283 030 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Presence Service Capability; Protocol Specification [3GPP TS 24.141 V7.0.0, modified and OMA-TS-Presence_SIMPLE-V1_0, modified]".

NOTE: The latest version in the V2.y.z series applies.

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

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

[19] ETSI TS 124 508 (V8.1.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); PSTN/ISDN simulation services Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR); Protocol specification (3GPP TS 24.508 version 8.1.0 Release 8)".

[20] ETSI TS 124 229 (V7.9.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229 version 7.9.0 Release 7)".

[21] ETSI TS 183 065 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networks(TISPAN); Customer Network Gateway Configuration Function; e3 Interface based upon CWMP".

NOTE: The latest version in the V2.y.z series applies.

[22] ETSI TS 124 503 (V8.4.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); TISPAN; IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP) Stage 3 [3GPP TS 24.229 (Release 7), modified] (3GPP TS 24.503 version 8.4.0 Release 8)".

[23] IETF RFC 2131: "Dynamic Host Configuration Protocol".

[24] ETSI TS 183 019 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment; User-Network Interface Protocol Definitions".

NOTE: The latest version in the V2.y.z series applies.

[25] Broadband Forum TR-069 Amendment 2: "CPE WAN Management Protocol v1.1"; Release 3; December 2007.

[26] Broadband Forum TR-098 Amendment 2: "Internet Gateway Device Data Model for TR-069"; Release 3; September 2008.

[27] ETSI TS 124 407 (V 8.0.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); TISPAN; PSTN/ISDN simulation services; Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR); Protocol specification (3GPP TS 24.407 version 8.0.0 Release 8)".

[28] IEEE 802.1X: "IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control".

[29] IETF RFC 3748: "The Extensible Authentication Protocol (EAP) specification".

[30] Wi-Fi Alliance: "WPA (includes WPA2) Pointer Document, version 3.0".

NOTE: Available at http://www.wi-fi.org.

[31] IEEE 802.11i (2004): "Enhanced security".

[32] Wi-Fi Alliance: "Wi-Fi Protected Setup Specification, version 1.0".

NOTE: Available at http://www.wi-fi.org.

[33] ETSI TS 183 041 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Messaging service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3: Protocol specifications [Endorsement of 3GPP TS 24.247 Release 6".

NOTE: the latest version in the V2.y.z series applies.

[34] ETSI TS 183 005 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Conference (CONF); Protocol specification".

NOTE: The latest version in the V2.y.z series applies.

[35] ETSI TS 183 016 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Malicious Communication Identification (MCID); Protocol Specification".

NOTE: The latest version in the V2.y.z series applies.

[36] ETSI TS 183 008 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR); Protocol specification".

NOTE: The latest version in the V2.y.z series applies.

[37] ETSI TS 124 238: "Universal Mobile Telecommunications System (UMTS); LTE; Session Initiation Protocol (SIP) based user configuration; Stage 3 (3GPP TS 24.238 version 8.1.0 Release 8)".

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

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

[40] ETSI TS 183 047 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN IMS Supplementary Services; Advice Of Charge (AOC)".

NOTE: The latest version in the V2.y.z series applies.

[41] ETSI TS 183 054 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Protocol specification Closed User Group (CUG)".

NOTE: The latest version in the V2.y.z series applies.

[42] ETSI TS 183 051 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Support of SMS and MMS over NGN IMS subsystem; Stage 3 [Endorsement of 3GPP TS 24.341 Release 7".

NOTE: The latest version in the V2.y.z series applies.

[43] ETSI TS 183 007 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services; Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR); Protocol specification".

NOTE: The latest version in the V2.y.z series applies.

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

[45] IETF RFC 3994: "Indication of Message Composition for Instant Messaging".

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

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

[48] IETF RFC 3515: "The Session Initiation Protocol (SIP) REFER Method".

[49] IETF RFC 3891: "The Session Initiation Protocol (SIP) Referred-By Mechanism".

[50] IETF RFC 3892: "The Session Initiation Protocol (SIP) "Replaces" Header".

[51] ETSI TS 183 028 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Common Basic Communication procedures; Protocol specification".

NOTE: The latest version in the V2.y.z series applies.

[52] ETSI TS 183 004 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Communication Diversion (CDIV); Protocol specification".

NOTE: The latest version in the V2.y.z series applies.

[53] ETSI TS 183 011 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Anonymous Communication Rejection (ACR) and Communication Barring (CB); Protocol specification".

NOTE: The latest version in the V2.y.z series applies.

[54] ETSI TS 183 029 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); PSTN/ISDN simulation services: Explicit Communication Transfer (ECT); Protocol specification".

NOTE: The latest version in the V2.y.z series applies.

[55] ETSI TS 183 010 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Signalling Control Protocol; Communication HOLD (HOLD) PSTN/ISDN simulation services; Protocol specification".

NOTE: The latest version in the V2.y.z series applies.

[56] UPnP™: "MediaRenderer:2 Device Template Version 1.01 (30 September 2008)".

NOTE: Available at http://www.upnp.org/specs/av/UPnP-av-MediaRenderer-v2-Device.pdf.

[57] UPnP™: "AVTransport:2 Service Template Version 1.01 (30 September 2008)".

NOTE: Available at http://www.upnp.org/specs/av/UPnP-av-AVTransport-v2-Service.pdf.

[58] UPnP™: "ContentDirectory:3 Service Template Version 1.01 (30 September 2008)".

NOTE: Available at http://www.upnp.org/specs/av/UPnP-av-ContentDirectory-v3-Service.pdf.

[59] UPnP™: "ScheduledRecording:2 Service Template Version 1.01 (30 September 2008)".

NOTE: Available at http://www.upnp.org/specs/av/UPnP-av-ScheduledRecording-v2-Service.pdf.

[60] ETSI ES 282 003 (V2.y.z): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS): Functional Architecture".

NOTE: The latest version in the V2.y.z series applies.

[61] ETSI TS 123 228: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsystem (IMS); Stage 2 (3GPP TS 23.228 version 8.8.0 Release 8)".

[62] Broadband Forum TR-104: "DSL Home™ Provisioning Parameters for VoIP CPE"; Release 1; September 2005.

[63] Broadband Forum TR-106 Amendment 2: "Data Model Template for TR-069 Enabled Devices"; Release 3; November 2008.

[64] Broadband Forum TR-135: "Data Model for TR-069 Enabled STB"; Release 3; December 2007.

[65] Broadband Forum TR-140 Issue 1.1: "TR-069 Data Model for Storage Service Enabled Devices"; Release 3; December 2007.

[66] IETF RFC 3193: "Securing L2TP using IPsec".

[67] ETSI TS 124 505 (V 8.0.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); TISPAN; PSTN/ISDN simulation services: Conference (CONF); Protocol specification (3GPP TS 24.505 version 8.0.0 Release 8)".

[68] ETSI TS 124 516 (V 8.0.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); TISPAN; PSTN/ISDN simulation services; Malicious Communication Identification (MCID); Protocol specification (3GPP TS 24.516 version 8.0.0 Release 8)".

[69] ETSI TS 124 447 (V 8.0.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); TISPAN; NGN IMS Supplementary Services; Advice Of Charge (AOC) (3GPP TS 24.447 version 8.0.0 Release 8)".

[70] ETSI TS 124 454 (V 8.0.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); TISPAN; PSTN/ISDN simulation services; Protocol specification Closed User Group (CUG) (3GPP TS 24.454 version 8.0.0 Release 8)".

[71] ETSI TS 124 430 (V 8.0.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); TISPAN; Presence Service Capability; Protocol Specification [3GPP TS 24.141 V7.0.0, modified and OMA-TS-Presence_SIMPLE-V1_0, modified] (3GPP TS 24.430 version 8.0.0 Release 8)".

[72] ETSI TS 124 441: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); TISPAN; Messaging service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3: Protocol specifications [Endorsement of 3GPP TS 24.247 Release 6] (3GPP TS 24.441 version 8.0.0 Release 8)".

[73] ETSI TS 123 521 (V 8.0.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Telecommunications and Internet converged Services and Protocols for Advanced Networks (TISPAN); Support of Short Message Service (SMS) over NGN IMS subsystem; Stage 2; [Endorsement of 3GPP TS 23.204 Release 7] (3GPP TS 23.521 version 8.0.0 Release 8)".

[74] ETSI TS 124 628 (V 8.2.0): "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 (3GPP TS 24.628 version 8.2.0 Release 8)".

[75] ETSI TS 124 604 (V 8.3.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Communication Diversion (CDIV) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.604 version 8.3.0 Release 8)".

[76] ETSI TS 124 611 (V 8.2.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Anonymous Communication Rejection (ACR) and Communication Barring (CB) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.611 version 8.2.0 Release 8)".

[77] ETSI TS 124 629 (V 8.2.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Explicit Communication Transfer (ECT) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.629 version 8.2.0 Release 8)".

[78] ETSI TS 124 610 (V 8.3.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Communication HOLD (HOLD) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.610 version 8.3.0 Release 8)".

[79] ETSI TS 124 605 (V 8.3.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Conference (CONF) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.605 version 8.3.0 Release 8)".

[80] ETSI TS 124 606 (V 8.1.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Message Waiting Indication (MWI)using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.606 version 8.1.0 Release 8)".

[81] ETSI TS 124 607 (V 8.2.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Originating Identification Presentation (OIP) and Originating Identification Restriction (OIR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.607 version 8.2.0 Release 8)".

[82] ETSI TS 124 608 (V 8.2.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Terminating Identification Presentation (TIP) and Terminating Identification Restriction (TIR) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.608 version 8.2.0 Release 8)".

[83] ETSI TS 124 616 (V 8.3.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Malicious Communication Identification (MCID)using IP Multimedia (IM) Core Network (CN) subsystem; Protocol specification (3GPP TS 24.616 version 8.3.0 Release 8)".

[84] ETSI TS 124 647 (V 8.1.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Advice Of Charge (AOC) using IP Multimedia (IM) Core Network (CN) subsystem; Protocol Specification (3GPP TS 24.647 version 8.1.0 Release 8)".

[85] ETSI TS 124 141 (V 8.3.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Presence service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3 (3GPP TS 24.141 version 8.3.0 Release 8)".

[86] ETSI TS 124 247 (V 8.2.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Messaging service using the IP Multimedia (IM) Core Network (CN) subsystem; Stage 3 (3GPP TS 24.247 version 8.2.0 Release 8)".

[87] ETSI TS 124 341 (V 8.1.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Support of SMS over IP networks; Stage 3 (3GPP TS 24.341 version 8.1.0 Release 8)".

[88] ETSI TS 124 654: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Closed User Group (CUG) using IP Multimedia (IM) Core Network (CN) subsystem, Protocol Specification (3GPP TS 24.654 version 8.2.0 Release 8)".

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] "UPnP Remote Access Transport Agent (RATA) Config:1 Service".

3 Definitions and abbreviations

3.1 Definitions

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

announcement: service related message sent to a user that can be of any type of media e.g. a voice message or a video-clip

transfer target: party which the communication is transferred to and which replaces the transferor in the communication

transferee: party which stays in the communication which is transferred

transferor: party that initiates the transfer of the active communication that it has with the transferee

3.2 Abbreviations

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

3DES-CBC	3'ple Data Encryption Standard - Cipher Block Chaining mode
3DES-CTR	3'ple Data Encryption Standard - CounTeR mode
AC	Access Controller
ACL	Access Control List
ACR	Anonymous Communication Rejection
AES	Advanced Encryption Standard
AES-CBC	Advanced Encryption Standard - Cipher Block Chaining mode
AES-CTR	Advanced Encryption Standard - CounTeR mode
AKA	Authentication and Key Agreement
ALG	Application Layer Gateway
AP	Access Point
ASP	Active Server Page(s)
B2BUA	Back-to-Back User Agent
CCRP	Compulsory Configuration Renewal Procedure
CD	Communication Deflection
CDIVN	Communication DIVersion Notification
CFB	Communication Forwarding on Busy user
CFNL	Communication Forwarding on Not Logged-in
CFNR	Communication Forwarding on No Reply
CFNRc	Communication Forwarding on subscriber Not Reachable
CFU	Communication Forwarding Unconditional
CHAP	Challenge Handshake Authentication Protocol
CLI	Customer Line Identifier
CND	Customer Network Device
CND-AtF	CND Attachment Function
CNDCP	CND Configuration Protocol
CNG	Customer Network Gateway
CNG-AtF	CNG-Attachment Function
CNG-AuF	CNG-Authentication Function
CNGCF	CNG Configuration Function
CNG-NFF	CNG-NAPT and Firewall Function
CNG-PPF	CNG-Plug and Play Function
CPN	Customer Premises Network
CWMP	CPE WAN Management Protocol
DHCP	Dynamic Host Configuration Protocol
DPD	Dead Peer Detection
DTMF	Dual-Tone Multi Frequency
EAP	Extensible Authentication Protocol
ECT	Explicit Communication Transfer
FQDN	Fully Qualified Domain Name
HEX	HEXadecimal
HMAC	Hash Message Authentication Code
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICB	Incoming Communication Barring
ICSI	IMS Communication Service Identifier
ID	IDentity
IETF	International Engineering Task Force
IKE	Internet Key Exchange
IMPU	IP Multimedia PUblic identity
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPsec	Internet Protocol secure transmission
IPTV	Internet Protocol TeleVision
IPv6	Internet Protocol (version 6)

Kbps	Kilo bits per second
L2TP	Layer 2 Tunnelling Protocol
LAN	Local Area Network
MAC	Media Access Control
MIME	Multipurpose Internet Mail Extensions
MMS	Multimedia Messaging Service
MODP	MODular exPonential Group
MWI	Message Waiting Indication
NACF	Network Access Configuration Function
NAPT	Network Address Port Translation
NAT	Network Address Translation
NGN	Next Generation Networks
OCB	Outgoing Communication Barring
OIP	Originating Identification Presentation
OIR	Originating Identification Restriction
PBC	Push Button Configuration
P-CSCF	Proxy Call Session Control Function
PIN	Personal Identification Number
PPP	Point to Point Protocol
PPPoE	Point-to-Point Protocol over Ethernet
QoS	Quality of Service
RA	Remote Access
RAC	Remote Access Client
RACS	Resource and Admission Control Subsystem
RADA	Remote Access Discovery Agent
RAS	Remote Access Server
RATA	Remote Access Transport Agent
RBAC	Role Based Access Control
RPC	Remote Procedure Call
RSA	Rivest-Shamir-Adleman encryption
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
SDP	Session Description Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SIT	SITuation
SMS	Short Message Service
SSID	Service Set IDentifier
STB	Set Top Box
TIP	Terminating Identification Presentation
TIR	Terminating Identification Restriction
TISPAN	Telecommunication and Internet converged Services and Protocols for Advanced Networking
UA	User Agent
UAC	User Agent Client
UAS	User Agent Server
UDP	Unicast Datagram Packet
UE	User Equipment
UPnP™	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
VoIP	Voice over IP
VPN	Virtual Private Networks
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access
XML	eXtensible Markup Language

4 Overview

The clause briefly describes applicability of the protocols discussed further in the present document to the reference points and functional entities defined in [1] and [2] as depicted in figure 4.1.

The IMS CND functions are described within the TS 185 006 [2] dedicated to Customer Network Devices.

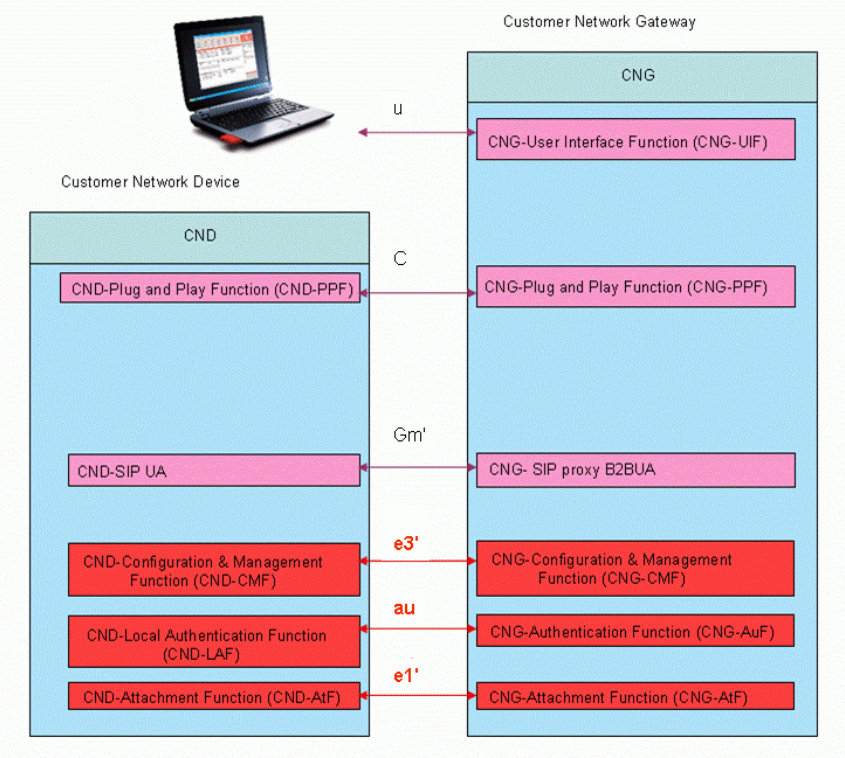


Figure 4.1: Customer Network Device and Customer Network Gateway usage of the local reference points

4.1 Protocols and Reference Points

The u reference point is described in clause 5.

The C reference point is described in clause 6, detailing procedures based on UPnP™.

The Gm' reference point is described in clause 7, detailing procedures based on SIP.

The e3' reference point is described in clause 8, detailing procedures based on HTTP.

The au reference point is described in clause 9, detailing procedures based on EAP.

The e1' reference point is described in clause 10, detailing procedures based on DHCP.

5 Procedures at the u Reference Point

NOTE: This clause is not elaborated in Release 2.

Content intended for this clause is procedures based on HTTP, for example HTTP authentication and access control.

Various methods for HTTP authentication will be elaborated and detailed. Examples of such authentication methods could be HTTP Cookie based authentication, HTTP Digest Authentication, HTTPS and/or HTTP Basic Authentication.

Solutions for access control will be elaborated and detailed. Examples of such solutions might be Role Based Access Control and/or the usage of Blacklists.

6 Procedures at the C Reference Point

6.1 Procedures for using UPnP™

6.1.1 Remote Access Functions

Architectural information is found in clauses 7.4 of TS 185 003 [1] and 8.4 in TS 185 006 [2].

The definition of the protocols on the C reference point conforms to the UPnP™ architecture. Using the C reference point for Remote Access (RA) is described in the following clauses: device discovery in clause 6.1.1.1 and performing actions (Push, Pull, etc.) in clauses 6.1.1.2 to 5.

NOTE: UPnP™ has defined architecture for UPnP™ Remote Access 1.0 including two entities called Remote Access Discovery Agent (RADA) and Remote Access Transport Agent (RATA). This is currently work in progress.

RADA functionality is located in the CNG-PPF and RATA functionality is found in the CNG-SIP Proxy B2BUA. Both are detailed in TS 185 003 [1].

For the utilization of the C reference point for Remote Access the precondition of a tunnel setup shall be fulfilled. The tunnel setup is performed using SIP signalling procedures on the Gm reference point. Further on security negotiation may be performed. These procedures are described in annex A "Remote Access Procedures".

The information regarding which CND or CND's that are registered within the home network (CPN) is discovered and maintained by RADA and is used to compile an Access Control List (ACL) managed by the CNG-SIP Proxy B2BUA.

To support the Remote Access there are two possible alternatives:

1) The CNG-SIP Proxy B2BUA should implement the complete B2BUA sub-block as described in TS 185 003 [1]. This is described in the upper part of figure 6.1.

2) The CNG-SIP Proxy B2BUA should implement the SIP Proxy sub-block and additionally the NGN side SIP UA termination of the B2BUA sub-block. This is described in the lower part of figure 6.1.

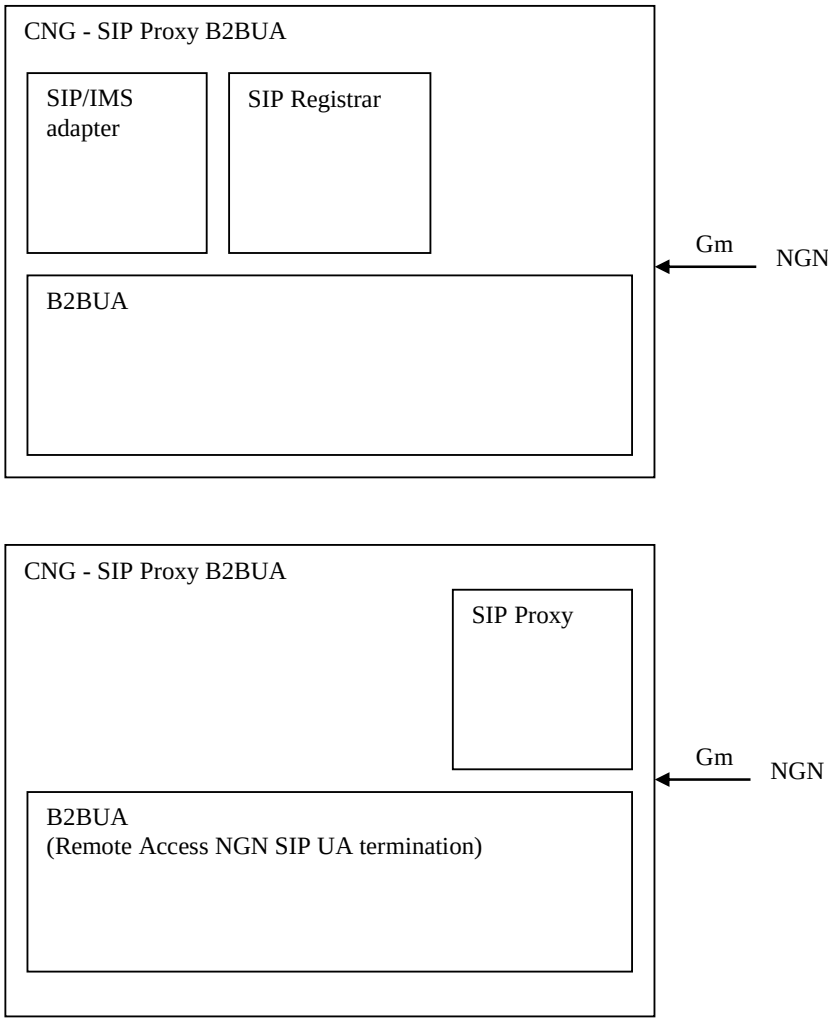


Figure 6.1: Possible Remote Access implementation alternatives in the CNG-SIP Proxy B2BUA

6.1.1.1 Device Discovery

The CNG-PPF collects available UPnP™ devices at a regular interval in accordance with UPnP™ Device Architecture 1.0 [6]. This is done using M-SEARCH and NOTIFY messages.

6.1.1.2 Push of Content

Over the C reference point this is an UPnP™ AVTransport; Play (as specified in [57]) action, etc. on home device providing UPnP™ MediaServer [5].

6.1.1.3 Pull of Content

Over the C reference point this is UPnP™ ContentDirectory; Browse (as specified in [58]) provided by the UPnP™ MediaServer [5] and AVTransport; Play (as specified in [57]) actions, etc., provided by the UPnP™ MediaRenderer [56].

6.1.1.4 Streaming of Content

Over C reference point this is behaving as the previous clause (Pull of content).

NOTE: Bandwidth allocation during tunnel setup in NGN Release 2 does not take into account the different directions, e.g. RTSP in both (sendrecv) and RTP in one (recvonly). Streaming Service Provider managed IPTV content from CPN is not specified in NGN Release 2.

6.1.1.5 Remote Control

Over C reference point this is UPnP™ ScheduledRecording::CreateRecordSchedule action, etc. on home device providing UPnP™ ScheduledRecording service [59].

7 Procedures at the Gm' Reference Point

7.1 General

In this clause, procedures at the Gm' reference points are specified both for non-IMS and IMS SIP devices.

- Non-IMS SIP device: devices complying with the definition of "Non-IMS capable device - SIP Device" in [2].
- IMS SIP device: devices complying to the definition of "IMS capable device" in [2], with the exception that in this context only IMS devices using unencrypted signalling (not using IMS AKA authentication) are valid.

NOTE: The references to procedures at the Gm reference point in this clause are valid for TISPAN NGN Release 2 implementations. For 3GPP Release 8 implementations, see the references indicated by annex B.

7.2 Procedures for non-IMS SIP devices

7.2.1 SIP Profiles

Non-IMS SIP devices complying with the present document could support IETF SIP to various degrees.

These levels of support are specified by using the concept of SIP Profiles.

Each SIP Profile corresponds to a defined functionality.

7.2.1.1 Basic Conversational Profile

Support for the Basic Conversational Profile is the minimum level of SIP support for a non-IMS SIP CND.

In the Basic Conversational Profile the following features shall be supported:

- Registration - registration procedures are detailed in clause 7.2.3.

  The support for the Registration functionality over the Gm' reference point corresponds to the support for registration, re-registration and de-registration functionalities over Gm as detailed in ES 283 003 [5].

- Call Initiation - call initiation procedures are detailed in clause 7.2.4.

  The support for the call initiation functionality over the Gm' reference point corresponds to the support for call initiation functionality over Gm as detailed in ES 283 003 [5].

- Call Release - call release procedures are detailed in clause 7.2.4.

  The support for the call release functionality over the Gm' reference point corresponds to the support for call release functionality over Gm as detailed in ES 283 003 [5].

- Call Modification - session modification are detailed in clause 7.2.4.

  The support for session modification functionality over the Gm' reference point corresponds to the support for session modification over Gm as detailed in ES 283 003 [5].

- Announcements - announcements are detailed in clause 7.2.4.7.

The support for announcements over the Gm' reference point corresponds to the support for Announcements over Gm as detailed in TS 183 028 [51].

7.2.1.2 Extended Conversational Profile

To be compliant with the Extended Conversational Profile support of the Basic Conversational Profile shall be extended with the following features:

- Indicating User Agent Capabilities in SIP - Procedures for indicating User Agent Capabilities are detailed in clause 7.2.8.
- The support for Indication User Agent Capabilities in SIP corresponds to the usage of RFC 3840 [18] for registration procedures.
- Capability Exchange (OPTIONS) - Procedures for Capability Exchange are detailed in clause 7.2.8.

  The support for Capability Exchange corresponds to the usage of the SIP OPTIONS method as defined in RFC 3261 [4].
- Messaging - Procedures for Messaging are detailed in clause 7.2.6.

  The support for Messaging corresponds to the procedures detailed in TS 183 041 Messaging Protocol Specification [33].
- DTMF Handling - DTMF procedures are detailed in clause 7.2.7.

  The support for the DTMF functionality over the Gm' reference point corresponds to the support for DTMF functionality over Gm as detailed in ES 283 003 [5].

7.2.1.3 Conversational Supplementary Services Profile

To be compliant with the Conversational Supplementary Services Profiles, support of the Basic Conversational Profile shall be extended with the following features:

- Service Activation/De-activation - Procedures for Service Activation/De-activation are detailed in clause 7.2.5.
- Communication Diversion - Procedures for Communication Diversion are detailed in clause 7.2.5.

  The support for Communication Diversion corresponds to the procedures specified by TS 183 004 [52].
- Communication Rejection - Procedures for Communication Rejection are detailed in clause 7.2.5.

  The support for Communication Rejection corresponds to the procedures detailed in TS 183 011 [53].
- Explicit Call Transfer - Procedures for Explicit Call Transfer are detailed in clause 7.2.5.

  The support for Explicit Call Transfer corresponds to the procedures detailed in TS 183 029 [54].
- Communication Hold - Procedures for Communication Hold are detailed in clause 7.2.5.

  The support for Communication Hold corresponds to the procedures detailed in TS 183 010 [55].
- 3 Party Conference - Procedures for 3 Party Conference are detailed in clause 7.2.5.

  The support for 3 Party Conference is based on procedures for Communication Hold and media mixing being performed locally in the CND.

- Message Waiting Indication - Procedures for Message Waiting Indication are detailed in clause 7.2.5.

  The support for Message Waiting Indication corresponds to the procedures detailed in TS 124 406 [13].

- Originating Identification - Procedures for Originating Identification are detailed in clause 7.2.5.

  The support for Originating Identification corresponds to the procedures detailed in TS 183 007 [43].

- Terminating Identification - Procedures for Termination Identification are detailed in clause 7.2.5.

  The support for Terminating Identification corresponds to the procedures detailed in TS 183 008 [36].

- Malicious Communication Identification - Procedures for Malicious Communication Identification are detailed in clause 7.1.5.10.

  The support for Malicious Communication Identification corresponds to the procedures detailed in TS 183 016 [35].

7.2.2 IETF RFC support

7.2.2.1 Basic Conversational Profile

In order to be compliant with the Basic Conversational Profiles, support of the following IETF specification shall be supported:

- RFC 3261 [4].

7.2.2.2 Extended Conversational Profile

In order to be compliant with the Extended Conversational Profile, support of the following IETF specifications shall be supported:

- RFC 3840 [18].
- RFC 3428 [44].

Additionally the following IETF specifications may be supported:

- RFC 2833 [17].
- RFC 3994 [45].

7.2.2.3 Conversational Supplementary Services Profile

In order to be compliant with the Conversational Supplementary Services Profile, the following IETF specifications shall be supported:

- RFC 3265 [47].
- RFC 3842 [46].
- RFC 3515 [48].
- RFC 3891 [49].
- RFC 3892 [50].

7.2.3 Registration

7.2.3.1 Registration of CND-SIP UA, general

The registration procedures for a CND-SIP UA shall be compliant with RFC 3261 [4], clause 10.

A CND-SIP UA can register a user identity (local or public) with its contact address at any time after it has learned its registration domain and acquired an IP address of the CND where it is executing.

However, the CND-SIP UA shall not initiate a new registration procedure if it has not received a final response from the registrar for the ongoing registration and if the previous REGISTER request has not timed out.

The user identity (local or public), registration domain (local or public) and optionally the registration port may be manually configured for the CND-SIP UA. It may also be configured automatically, for example by using the e3' reference point.

HTTP Digest Authentication should be used as authentication method when registering the CND-SIP UA.

If so, authentication credentials (user and password) shall be made available to the CND-SIP UA in one of the following ways:

1) pre-configuration;

2) provisioning (auto-configuration);

3) manual configuration.

The CND-SIP UA shall send its REGISTER requests to the registration port, if specified by configuration. If no registration port is specified the CND-SIP UA shall send its REGISTER requests to the SIP default port values as specified in RFC 3261 [4].

On sending a REGISTER request, the CND-SIP UA shall populate the header fields as follows:

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

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

c) a Contact header set to include SIP URI(s) containing the IP address of the CND-SIP UA in the hostport parameter or FQDN;

d) a Via header set to include the IP address or FQDN of the non-IMS SIP UA in the sent-by field;

e) a Request-URI set to the SIP URI containing the registration domain.

On receiving the 200 (OK) response to the REGISTER request, the CND-SIP UA shall store the expiration time of the registration for the user identity found in the To header value.

It should be possible to de-register the CND-SIP UA by manual user interaction, or at normal termination of the CND-SIP UA.

7.2.3.2 Registration of CND-SIP UA, using local SIP-URI

The local user identity field should contain a value that is administered by the CNG-SIP Proxy B2BUA and the value of the registration domain field should be the registration domain handled by the CNG-SIP Proxy B2BUA.

When a CND-SIP UA is registered in the CNG-SIP Proxy B2BUA with a local identity it will be available for local services.

If the local SIP account provided by the CNG-SIP Proxy B2BUA is associated with an IMS identity, the CND-SIP UA will also be available for NGN services. This association could be done by configuration in the CNG-SIP Proxy B2BUA.

If authentication procedures applies at registration of the CND-SIP UA locally at the CNG-SIP B2BUA, the HTTP Digest method, as specified in RFC 3261 [4], shall be.

The CND-SIP UA shall not use the same Contact value to register multiple local SIP-URIs.

7.2.3.3 Registration of CND-SIP UA, using public SIP-URI not preconfigured in CNG

The public user identity field should contain a value corresponding to a service provided by the NGN side of the CNG.

The value of the registration domain field should be that of the service provided by the NGN side of the CNG.

When a CND-SIP UA is registered in the CNG-SIP Proxy B2BUA with a public identity that is not pre-configured in the CNG, the CNG should forward the registration request according to the following principles:

(i) If the CNG-SIP Proxy B2BUA is associated with a P-CSCF it may forward all registration requests to that server in a transparent fashion. In parallel the CNG-SIP Proxy B2BUA may create a local registration entry for the CND-SIP UA in order to enable local services for the CND-SIP UA. Any peering decisions are made by the NGN.

(ii) As an alternative (optionally triggered by configuration) the CNG-SIP Proxy B2BUA should forward the registration requests to the destination specified in the Request-URI of the REGISTER request sent by the CND-SIP UA. In this case the CND-SIP UA should not be included in the local services (such as local communication, QoS or admissions control).

7.2.3.4 Registration of CND-SIP UA, using public SIP-URI that is pre-configured in CNG

The public user identity field should contain a value corresponding to a service provided by the NGN side of the CNG.

The value of the registration domain field should be that of the service provided by the NGN side of the CNG.

When a CND-SIP UA is registered in the CNG-SIP Proxy B2BUA with a public identity that is pre-configured in the CNG the following principles apply:

(i) If the CNG-SIP Proxy B2BUA is a SIP Proxy it should forward the REGISTER request to the destination specified by the Request-URI. It should at the same time create a local registration entry for the CND-SIP UA.

(ii) If the CNG-SIP Proxy B2BUA is a B2BUA it should refresh its public registration with new data, for example if new capabilities are added by the CND-SIP UA. At the same time it should create a local registration entry for the CND-SIP UA.

7.2.4 Basic Call

The procedures for a CND-SIP UA related to Basic Calls are compliant with the following clauses within RFC 3261 [4]:

- clause 7
- clause 8
- clause 9
- clause 12
- clause 13
- clause 14
- clause 15
- clause 17
- clause 18
- clause 19

- clause 20
- clause 21

7.2.4.1 Call Initiation

7.2.4.1.1 Outgoing call

On sending an INVITE request, the CND-SIP UA shall populate the header fields as follows:

a) a From header set to the SIP URI that contain the local user identity of the caller (registered in the CNG-SIP B2BUA) or in cases where privacy is required, the CND-SIP UA shall set the From header display name to "Anonymous" and the URI shall be set to a meaningless value, such as sip:anonymous@example.com;

b) a To header set to the SIP URI that contains the public or local user identity of the callee;

c) a Contact header set to include SIP URI(s) containing the IP address of the CND-SIP UA in the hostport parameter or FQDN;

d) a Via header set to include the IP address or FQDN of the non-IMS SIP UA in the sent-by field;

e) a Request-URI set to the SIP URI containing the user identity of the callee (local or public) and a domain part either specified by the caller or the domain of the CNG-SIP B2BUA.

HTTP Digest authentication mechanism may be used for outgoing Call Initiation over Gm'.

An INVITE request generated by a CND-SIP UA shall contain a SDP offer and at least one media description. The SDP offer shall reflect the calling user's capabilities and user preferences for the session. The CND-SIP UA shall order the SDP offer with the most preferred codec listed first.

When the CNG-SIP B2BUA receives an INVITE from the CND-SIP UA addressed to the domain of the CNG-SIP B2BUA, it shall first check if the caller contained in the From-header is registered (either explicitly or implicitly) within the CNG-SIP B2BUA registrar. If an explicitly stated (not anonymous) caller is not registered, the CNG-SIP B2BUA shall reject the call by sending a 403 Forbidden response.

Furthermore, and in case of anonymous calls, the CNG-SIP B2BUA should additionally use any of the methods below to verify the caller:

(i) If HTTP Digest authentication is used for the INVITE the CNG-SIP B2BUA may use the user part of the authentication mechanism to verify the user.

(ii) If no authentication mechanism is used, the CNG-SIP B2BUA should check if the Contact information corresponds to information in the contact list found in the CNG-SIP B2BUA registrar for the caller.

If the CNG-SIP B2BUA is unable to verify the caller, it should reject the call by sending a 403 Forbidden response.

After verification of the caller, the CNG-SIP B2BUA should check if the callee is registered locally within the CNG-SIP B2BUA registrar. If so, the procedures of 7.2.4.1.2 shall apply.

If it is not a local call, the CNG-SIP B2BUA should check if the local identity of the caller is associated with a public identity.

If this is the case the CNG-SIP B2BUA shall initiate a call to the NGN on the behalf of the local caller using the public identity and following the procedures specified for the Gm reference point. In this process the CNG-SIP B2BUA shall initiate media forwarding from the NGN to the CPN in order to be able to receive early media from the NGN.

If the local identity of the caller is not associated with a public identity (either explicitly by configuration or implicitly by following the registration procedures as specified in 7.2.3.3 (i) or 7.2.3.4 (i), the CNG-SIP B2BUA shall reject the call by sending a 403 Forbidden response.

When the CNG-SIP B2BUA receives an INVITE from the CND-SIP UA addressed to a domain other than it own it may forward the INVITE request to its P-CSCF in a transparent fashion. Any peering decisions will be made by the NGN.

When receiving a provisional response from the NGN, the CNG-SIP B2BUA shall send the provisional response on Gm' (where reliability of provisional responses is not required). On Gm the CNG-SIP B2BUA implements the full IMS UE procedures and thus sends PRACK to the NGN.

Upon receiving provisional responses containing early media streams from the NGN, the CNG-SIP B2BUA shall set up the media forwarding in the CNG if preconditions are met. A port shall be allocated for reception of media from the CPN and port forwarding shall be set up by using the CNG-NFF.

Upon reception of a final response the CNG-B2BUA shall send a final response with the same response code on Gm' to the calling CND-SIP UA.

If the final response is 200 OK containing an SDP answer, the CNG-SIP B2BUA should follow the procedures specified in TS 124 229 [20], clause 6. Also the CNG-SIP B2BUA should initiate media port forwarding from the CPN to the NGN.

Upon reception of multiple 200 OK on Gm the CNG-SIP B2BUA terminates these multiple dialogs according to the procedures specified for Gm specified in TS 124 229 [20], clause 5.1.3. The reception of the multiple 200 OK does in this case not initiate any activity by the CNG-SIP B2BUA on the Gm' reference point.

Upon receiving the final response, the CND-SIP UA shall send the ACK request according to the procedures specified in RFC 3261 [4].

7.2.4.1.2 Internal call between CND-SIP UAs

The user identity field or the Request-URI contains the value of the called user from the CND-SIP UA, in this case a user that is defined for the registration domain administered by the CNG-SIP B2BUA.

The value of the domain field of the Request-URI should be the value of the registration domain handled by the CNG-SIP B2BUA.

When the CNG-SIP B2BUA receives the INVITE addressed to the local user identity, it recognizes that the called user is registered in the local registrar associated with the CNG-SIP B2BUA. The call shall then be routed according to the registered contact list for the called local user identity.

The CNG-SIP B2BUA shall not route the internal call via the NGN.

If the call is locally forked, the same forwarding mechanisms of responses apply as specified for a forking proxy in RFC 3261 [4]. Details are contained in RFC 3261 [4], clause 16.7, steps 5 and 6, excluding the header specific parts of the text and the parts dealing with hop-by-hop delivery.

When the calling CND-SIP UA receives the final response it shall send the ACK request according to the procedures specified in RFC 3261 [4].

Since the call is local, the media will be locally routed and no media forwarding needs to be set up by using the CNG-NFF.

7.2.4.1.3 Incoming Call Initiation, locally non-forked call

The procedures for incoming calls from NGN to the CNG-SIP B2BUA are the procedures specified for the Gm reference point in ES 283 003 [5].

When receiving an incoming INVITE at the Gm reference point, the CNG-SIP B2BUA checks the Request-URI to determine which public identity is being called.

The CNG-SIP B2BUA proceeds by determining which local identity is associated with the public identity. In the locally non-forked case only one local identity will be associated with the public identity.

Based on the SDP offer contained in the incoming INVITE, the CNG-SIP B2BUA shall set up media forwarding from CPN to NGN.

The CNG-SIP B2BUA gets the contact list for the local identity from the registrar, which in the locally non-forked case only will consist of one entry.

The CNG-SIP B2BUA then sends an INVITE to the contact associated with the local identity.

On sending an INVITE request, the CNG-SIP B2BUA shall populate the header fields as follows:

a) a From header set to the value of the incoming INVITE from NGN to the CNG-SIP B2BUA;

b) a To header set to the value of the incoming INVITE from NGN to the CNG-SIP B2BUA;

c) a Contact header set to a value generated from the local URI found by the CNG-SIP B2BUA;

d) a Via header set to the IP address or FQDN of the CPN side of the CNG-SIP B2BUA;

e) a Request-URI set to the SIP URI retrieved from the contact list for the local user.

The INVITE sent from the CNG-B2BUA to the CPN shall contain a media offer containing the media port(s) allocated by the CNG-SIP B2BUA upon reception of the incoming INVITE from the NGN.

The CND-SIP UA shall generate provisional responses according to the procedures defined in RFC 3261 [4]. Upon reception the CNG-SIP B2BUA will send a provisional response with the same response code to the NGN on the Gm reference point, following the procedures specified in ES 283 003 [5].

The CND-SIP UA shall generate the final response according to the procedures defined in RFC 3261 [4]. Upon reception the CNG-SIP B2BUA will send a final response with the same response code to NGN on the Gm reference point, following the procedures specified in ES 283 003 [5].

While receiving an SDP answer in either a provisional response or a final response the CNG-SIP B2BUA shall set up media forwarding to be able to transfer media from the NGN. Ports allocated by the CNG-SIP B2BUA for an early SIP dialog may be re-used at confirmation of the dialog.

Upon reception of the ACK on Gm from the NGN, the CNG-SIP B2BUA shall initiate a corresponding ACK request on Gm' following the procedures specified in RFC 3261 [4].

7.2.4.1.4 Incoming Call Initiation, locally forked call

The procedures for incoming calls from NGN to the CNG-SIP B2BUA are the procedures specified for the Gm reference point ES 283 003 [5].

When receiving an incoming INVITE at the Gm reference point, the CNG-SIP B2BUA checks the Request-URI to determine which public identity is being called.

The CNG-SIP B2BUA proceeds by determining which local identity is associated with the public identity. In the locally forked case multiple local identities may be associated with the public identity.

For each of these local identities the CNG-SIP B2BUA gets the contact list from the registrar, which in the locally forked case may consist of multiple entries, creating a super-set of these contact lists.

The CNG-SIP B2BUA then sends an INVITE to each of the contacts in the above super-set.

For each INVITE request, the CNG-SIP B2BUA shall populate the header fields as follows:

a) a From header set to the value of the incoming INVITE from NGN to the CNG-SIP B2BUA;

b) a To header set to the value of the incoming INVITE from NGN to the CNG-SIP B2BUA;

c) a Contact header set to a value generated from the local URI found by CNG-SIP B2BUA;

d) a Via header set to the IP address or FQDN of the CPN side of the CNG-SIP B2BUA;

e) a Request-URI set to the SIP URI retrieved from the contact list for the local user.

The same routing mechanisms of the SIP responses to the forked call applies as specified for a forking proxy in RFC 3261 [4]. Details are contained in RFC 3261 [4], clause 16.7, steps 5 and 6, excluding the header specific parts of the text and the parts dealing with hop-by-hop delivery.

Given the forking mechanisms as specified above; for the provisional and final responses to be sent to NGN; the CNG-B2BUA will initiate sending these responses according to the procedures specified for Gm in ES 283 003 [5].

After receiving an SDP answer in a final response the CNG-SIP B2BUA shall set up media forwarding to be able to receive media from the NGN. The CNG-SIP B2BUA shall also set up media forwarding based on the SDP offer contained in the original incoming INVITE to be able to transfer media from the CPN.

Upon reception of the ACK on Gm from the NGN, the CNG-SIP B2BUA shall initiate a corresponding ACK request on Gm' following the procedures specified in RFC 3261 [4].

NOTE: This means early media from CND-SIP UAs will not be supported for locally forked incoming calls.

7.2.4.2 Call Release of session during session establishment

When sending a CANCEL request on Gm' the CND-SIP-UA shall apply the procedures specified in RFC 3261 [4], clauses 9 and 9.1.

Upon receiving a CANCEL request on Gm' the CND-SIP-UA shall apply the procedures specified in RFC 3261 [4], clauses 9 and 9.1.

Upon receiving a CANCEL request on Gm' the CNG-SIP B2BUA shall apply the procedures specified in clauses 9 and 9.2. The CNG-SIP B2BUA shall free any allocated media resources and generate a corresponding CANCEL request on Gm according to the procedures specified in TS 124 503 [22], clauses 5.1.2A and 5.1.2A.1.

Upon receiving a CANCEL request on the Gm reference point the CNG-SIP B2BUA shall apply the procedures specified in TS 124 503 [22], clauses 5.1.2A and 5.1.2A.2. The CNG-SIP B2BUA shall free any allocated media resources and generate a corresponding CANCEL request on the Gm' reference point according to the procedures specified in RFC 3261 [4], clauses 9 and 9.1.

7.2.4.3 Call Release of existing session

When sending a BYE request on Gm' the CND-SIP-UA shall apply the procedures specified in RFC 3261 [4], clauses 15.1 and 15.1.1.

Upon receiving a BYE request on Gm' the CND-SIP-UA shall apply the procedures specified in RFC 3261 [4], clauses 15.1 and 15.1.2.

Upon receiving a BYE request on Gm' the CNG-SIP B2BUA shall apply the procedures specified in clauses 15.1 and 15.1.2. The CNG-SIP B2BUA shall free resources associated with the session and generate a corresponding BYE request on Gm according to the procedures specified in TS 124 503 [22], clauses 5.1.2A and 5.1.2A.1.

Upon receiving a BYE request on the Gm reference point the CNG-SIP B2BUA shall apply the procedures specified in TS 124 503 [22], clauses 5.1.2A and 5.1.2A.2. The CNG-SIP B2BUA shall free resources associated with the session and generate a corresponding BYE request on the Gm' reference point according to the procedures specified in RFC 3261 [4], clauses 15.1 and 15.1.1.

7.2.4.4 Call Modification

When generating a re-INVITE on Gm' the CND-SIP-UA shall apply the procedures specified in RFC 3261 [4], clauses 14 and 14.1.

Upon receiving a re-INVITE on Gm' the CND-SIP-UA shall apply the procedures specified in RFC 3261 [4], clauses 14 and 14.2.

Upon receiving a re-INVITE on Gm' the CNG-SIP B2BUA shall apply the procedures specified in clauses 14 and 14.2. The CNG-SIP B2BUA shall generate a corresponding re-INVITE request on Gm according to the procedures specified in TS 124.229 [20], clauses 5.1.2A and 5.1.2A.1 in combination with the TS 124.229 [20] endorsement of RFC 3261 [4], clauses 14 and 14.1. Upon completion of the re-INVITE transactions, the CNG-SIP B2BUA shall add, free or modify media resources according to the negotiated result.

Upon receiving a re-INVITE on Gm the CNG-SIP B2BUA shall apply the procedures specified in TS 124.229 [20], clauses 5.1.2A and 5.1.2A.2 in combination with the TS 124 229 [20] endorsement of RFC 3261 [4], clauses 14 and 14.2. The CNG-SIP B2BUA shall generate a corresponding re-INVITE request on Gm' according to the procedures specified in RFC 3261 [4], clauses 14 and 14.1. Upon completion of the re-INVITE transactions, the CNG-SIP B2BUA shall add, free or modify media resources according to the negotiated result.

7.2.4.5 Announcements

The following announcements methods, as specified by TS 183 028 [51], shall be supported for the non-IMS CND-SIP UAs:

- Announcement received by the service during an established communication session, using the existing media stream.
- Announcement received when a communication request is rejected, by the method where the service accepts the communication requests using the established session for sending an in-band announcement. Then the service terminates the dialog with the originating user.
- Announcement during the release of a communication session where the service uses the existing media stream or changes to new media for sending the announcement.

To support the above Announcement methods, the CND-SIP UA and the CNG-SIP B2BUA shall follow the procedures specified in clauses 7.2.4.2 to 7.2.4.4.

7.2.5 Conversational Supplementary Services

7.2.5.1 Activation/deactivation of services

NOTE: Activation/deactivation of services is not elaborated in Release 2.

7.2.5.2 Communication Diversion

The following Communication Diversion services, as specified in TS 124 504 [8] will be supported on the Gm' reference point: CFU, CFB, CFNR, CD, CFNL and CFNRc.

The following Communication Diversion service, as specified in TS 124 504 [8] will not be supported in the Gm' reference point: CDIVN.

When the CND-SIP UA is originating a call the CND-SIP UA and the CNG-SIP B2BUA shall follow the procedures specified in clause 7.1.4. If communication diversion has occurred on the served network side, the CNG-SIP B2BUA may receive a 181 according to the procedures specified in TS 124 504 [8]. The CNG-SIP B2BUA shall then send corresponding 181 response on the CPN side following the procedures for SIP UA specified in RFC 3261 [4]. Headers required for the 181 response on Gm according to table 4.4.1.1 of TS 124 504 [8] should not be included in the 181 response on the CPN side, with the exception of the History-Info header, specified in RFC 4244 [38], which may be included. The information given by the History-Info header may be displayed by the CND-SIP UA.

When the CND-SIP UA is the diverted to party, the procedures according to clause 7.1.4.

When the CND-SIP UA is the diverting party, the procedures according to clause 7.1.4 shall apply. For the Communication Deflection service the CND-SIP UA shall send a 302 response according to RFC 3261 [4], clause 13.3.1.2. Upon reception of the 302 Moved Temporarily from the CND-SIP UA, the CNG-SIP B2BUA shall generate a corresponding 302 response on the CPN side according to clause 4.5.2.16 of TS 124 504 [8]. The CNG-SIP B2BUA shall inspect the Contact header of the 302 response received on the CPN side and if it represent a local SIP-URI hosted by the CNG-SIP B2BUA, the CNG-SIP B2BUA shall replace this value with the value of the IMS IMPU that is associated to the local SIP-URI in the 302 response sent on the NGN side.

7.2.5.3 Communication Rejection

The following Communication Rejection services, as specified in TS 124 411 [9] will be supported on the Gm' reference point: ICB, OCB and ACR.

When the CND-SIP UA is originating a call the CND-SIP UA and the CNG-SIP B2BUA shall follow the procedures specified in clause 7.1.4:

- If OCB or ICB has occurred, the CNG-SIP B2BUA will receive a 603 (Decline) response according to the procedures specified in TS 124 411 [9]. The CNG-SIP B2BUA shall then send corresponding 603 response on the CPN side following the procedures for SIP UA specified in RFC 3261 [4].

- If ACR has occurred, the CNG-SIP B2BUA will receive a 433 (Anonymity Disallowed) response according to the procedures specified in TS 124 411 [9]. The CNG-SIP B2BUA shall then send a 603 (Decline) response on the CPN side following the procedures for SIP UA specified in RFC 3261 [4].

7.2.5.4 Explicit Communication Transfer

The Explicit Communication Transfer service is supported for the scenario, where one CND-SIP UA within the CPN has the role of a transferor, a transferee, or a transfer target. The other roles will be executed by endpoints outside the CPN for this scenario.

7.2.5.4.1 CND-SIP UA is transferor

When the CND-SIP UA has the role of the transferor it shall hold the dialog established with the transferee by applying the procedures specified in clause 7.2.5.5.

If the CND-SIP UA has established a dialog also with the transfer target, it shall hold that dialog by applying the procedures specified in clause 7.2.5.5.

Then the CND-SIP UA shall issue a REFER request, as specified by RFC 3515 [48], in the original communications dialog with the transferee.

For that REFER request the following applies:

- The request URI shall contain the SIP URI of the transferee as received in the Contact header field.
- The Refer-To header field shall indicate the public address of the transfer target.
- If the transferor UE has a consultation communication with the transfer target, a Replaces header field parameter shall be added to the Refer-To URI according to RFC 3891 [49] together with a Require: replaces header.
- A Referred-By header field, as specified by RFC 3892 [50], may be added to indicate the identity of the transferor.

When the CNG-SIP B2BUA receives the REFER on the CPN side, it shall generate a corresponding REFER on the NGN side. If a Replaces header is present, the information related to the CPN-side dialog shall be replaced with the values of the corresponding dialog on the NGN side. If a Referred-By header field is present, the local URI of the transferor shall be replaced by the associated public URI in the CNG-SIP B2BUA.

After reception of a 202 (Accepted) response for the REFER, the CND-SIP UA 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 CND-SIP UA may terminate the original communication with the transferee, by sending a BYE message on the original dialog.

7.2.5.4.2 CND-SIP UA is transferee

When the CNG-SIP B2BUA receives a REFER request on the NGN side, it shall apply the procedures specified in TS 125.529 [10] for an UE having the role of a transferee. The CNG-SIP B2BUA shall generate a corresponding REFER on the CPN side, keeping the Referred-By as received on the NGN side.

When a REFER request is received within the dialog to be transferred, the CND-SIP UA shall apply normal REFER handling procedures according to RFC 3515 [48] and RFC 3892 [50].

If the CND-SIP UA accepts the REFER by sending a 202 (Accepted) response, the CND-SIP UA should, within the dialog to be transferred, send notifications of how the communication setup towards the transfer target is progressing.

7.2.5.4.3 CND-SIP UA is transfer target

The CND-SIP UA and the CNG-SIP B2BUA applies the procedures specified in clause 7.2.4.

The CNG-SIP B2BUA implements the UE when having the role of a transfer target, as specified in TS 124 529 [10]. When the CNG-SIP B2BUA receives a Replaces header on the NGN side, it shall generate a corresponding Replaces header on the CPN side but with the values matching the dialog on the CPN side that is associated with the replaced dialog on the NGN side.

7.2.5.5 Communication Hold

The CND-SIP UA and the CNG-SIP B2BUA shall follow the procedures specified in clause 7.2.4.4.

In addition the CND-SIP UA shall apply the following procedures, in accordance with RFC 3264 [39], when holding or resuming a media stream:

If individual media streams are affected:

- for each media stream that shall be held, the invoking CND-SIP UA shall generate a new SDP offer that contains:
  - an "inactive" SDP attribute if the stream was previously set to "recvonly" media stream; or
  - a "sendonly" SDP attribute if the stream was previously set to "sendrecv" media stream;
- for each media stream that shall be resumed, the invoking CND-SIP UA shall generate a new SDP offer that contains:
  - a "recvonly" SDP attribute if the stream was previously an inactive media stream; or
  - a "sendrecv" SDP attribute if the stream was previously a sendonly media stream, or the attribute may be omitted, since sendrecv is the default.

If all the media streams in the SDP are affected:

- for the media streams that shall be held, the invoking CND-SIP UA shall generate a session level direction attribute in the SDP that is set to:
  - "inactive" if the streams were previously set to "recvonly" media streams; or
  - "sendonly" if the streams were previously set to "sendrecv" media streams;
- for the media streams that shall be resumed, the invoking CND-SIP UA shall generate a session level direction attribute in the SDP that is set to:
  - "recvonly" if the streams were previously inactive media streams; or
  - "sendrecv" if the streams were previously sendonly media streams, or the attribute may be omitted, since sendrecv is the default.

Upon reception of this re-INVITE from the CND-SIP UA, the CNG-SIP B2BUA shall generate a corresponding re-INVITE on the NGN side, applying the procedures specified in clause 4.5.2.1 of TS 124.410 [11].

Upon reception of a re-INVITE on the NGN side, the CNG-SIP B2BUA shall generate a corresponding re-INVITE on the CPN side, applying the procedures specified in clause 7.1.4.5. On the NGN the CNG-SIP B2BUA shall comply with clause 4.5.2.9 of TS 124 410 [11].

7.2.5.6 Conference (3-Party)

When the CND-SIP UA has the role of the initiator of a 3-party conference it shall establish a call, hereby referred to as the primary call, with the first conference participant according to the procedures specified in clause 7.2.4.

After establishment of the primary call, it shall be put on hold by applying the procedures specified in clause 7.2.5.5.

The CND-SIP UA acting as the initiator shall then establish a call, hereby referred to as the secondary call, with the second conference participant according to the procedures specified in clause 7.2.4.

After establishment of the secondary call, to enter conference state the CND-SIP UA acting as the initiator shall put the primary call off-hold by applying the procedures specified in clause 7.2.5.5. At the same time, media mixing locally in the CND shall be initiated.

If a conference participant terminates the call, the procedures specified in clause 7.2.4.3 applies for the call. The local media mixing shall then be terminated by the CND-SIP UA acting as the conference initiator. After these procedures are completed, only one basic call is remaining between the conference initiator and one of the conference participants.

If the CND-SIP UA acting as the conference initiator terminates the call, the procedures specified in clause 7.2.4.3 may be applied for both the primary and the secondary call. As an alternative, the CND-SIP UA may establish a call between the two participants by initiating an Explicit Communication Transfer, acting as a transferor. The ECT shall be initiated by applying the procedures specified in clause 7.2.5.4.1. Before initiating Explicit Communication Transfer, the local media mixing shall be terminated by the conference initiator CND-SIP UA.

7.2.5.7 Message Waiting Indication

The CND-SIP UA may implement the role of a MWI Subscriber, as defined in RFC 3842 [46] and RFC 3265 [47].

As an alternative, the CND-SIP UA may implement handling of unsolicited notifications, i.e. supporting an implicit subscription of the message-summary event package. In this case, the CNG-SIP B2BUA will issue the subscription on behalf of the CND-SIP UA(s) on the NGN side. The local registration of the CND-SIP UA to the local identity hosted by the CNG-SIP B2BUA will then trigger the implicit subscription.

If the CND-SIP UA subscribes explicitly for status information changes of a message account, it shall generate a SUBSCRIBE request in accordance with RFC 3265 [47] and RFC 3842 [46]. Depending on service provisioning the CND-SIP UA will address the SUBSCRIBE request either to the subscriber's local user identities or to the public service identity of the message account. If the CND-SIP UA addresses the SUBSCRIBE request to the local user identity hosted by the CNG-SIP B2BUA, the CNG-SIP B2BUA shall generate a corresponding request on the NGN side, using the public identity that is associated with the local identity of the SUBSCRIBE request that was received on the CPN side.

For either type of subscription, the CND-SIP UA shall implement the "application/simple-message-summary" content type as described in RFC 3842 [46].

If the CNG-SIP B2BUA subscribes to the message-summary event package on behalf of the CND-SIP UA, the CNG-SIP B2BUA implements the role of a MWI Subscriber User Agent, as specified in TS 124 406 [13] on the NGN side.

As the CNG-SIP B2BUA receives a notification on the NGN side, it shall generate corresponding notification on the CPN side for the CND-SIP UA(s) registered with the local identity that is associated with the public identity on the NGN side for which the CNG-SIP B2BUA has issued the subscription.

7.2.5.8 Originating Identification

The following Originating Identification services, as specified in TS 124 407 [27] will be supported on the Gm' reference point: OIP and OIR.

To support OIP the CND-SIP UA and the CNG-SIP B2BUA shall follow the procedures specified in clause 7.2.4.

To support OIR when originating a call the CND-SIP UA shall use the From display-name value "Anonymous" together with a meaningless URI as specified in clause 8.1.1.3, in RFC 3261 [4] when originating a call. When the CNG-SIP B2BUA receives an INVITE on the CPN side containing a From header where the display-name part equals "Anonymous", the CNG-SIP B2BUA shall follow the procedures specified in clause 4.5.2.1 of TS 124 407 [27].

To support OIR when receiving an INVITE from the NGN side, the CNG-SIP B2BUA shall follow the procedures specified in clause 4.5.2.12 of TS 124 407 [27]. If the caller identity is restricted, the CNG-SIP B2BUA shall generate the INVITE on the CPN using the From display-name value "Anonymous" together with a meaningless URI as specified in clause 8.1.1.3, in RFC 3261 [4].

When receiving an INVITE from the CNG-SIP B2BUA, the CND-SIP UA may present information contained in the From header to the user.

7.2.5.9 Terminating Identification

The following Terminating Identification services, as specified in TS 124 508 [19] will be supported: TIP and TIR, when CND-SIP UA is the terminator of the call.

The following Terminating Identification services, as specified in TS 124 508 [19] will not be supported: TIP and TIR, when CND-SIP UA is the originator of the call.

The CND-SIP UA and the CNG-SIP B2BUA shall follow the procedures specified in clause 7.1.4. Additionally, to support TIP and TIR when receiving an INVITE from the NGN side, the CNG-SIP B2BUA shall follow the procedures specified in clause 4.5.2.12 of TS 124 508 [19], when generating non-100 responses on the NGN side.

7.2.5.10 Malicious Communication Identification

To support Malicious Communication Identification, the CND-SIP UA and the CNG-SIP B2BUA shall follow the procedures specified in clause 7.2.4.

7.2.6 Messaging

The following Messaging service is supported: page-mode messaging.

The following Messaging services are not supported: session-mode messaging, session-mode messaging conference.

The CND-SIP UA shall send a page-mode message to another participant or a server by using a SIP MESSAGE request as defined in RFC 3428 [44]. The CND-SIP UA may include in a MESSAGE request an isComposing status message as defined in RFC 3994 [45]. The CND-SIP UA shall stop transmitting isComposing status messages if it receives a 415 (Unsupported Media Type) status code in a response to a MESSAGE request containing the status indication.

When the CND-SIP UA receives a page-mode message it shall apply the procedures specified in RFC 3428 [44]. If the SIP MESSAGE request contains an isComposing status message, the CND-SIP UA shall apply the procedures specified in RFC 3994 [45].

When the CNG-SIP B2BUA receives a SIP MESSAGE request on the CPN side, it shall generate a corresponding SIP MESSAGE request of the NGN side, following the procedures specified in RFC 3428 [44] and clause 5.1.2A.1 of TS 124.229 [20].

When the CNG-SIP B2BUA receives a MESSAGE request on the NGN side, it shall apply the procedures specified in RFC 3428 [44] and clause 5.1.2A.2 of TS 124 229 [20]. The CNG-SIP B2BUA shall generate a corresponding SIP MESSAGE request on the CPN side, following the procedures specified in RFC 3428 [44].

7.2.7 DTMF

The CND-SIP UA should implement the MIME subtype "telephone-event" in the "m=" media descriptor in the SDP for audio media flows that support both audio codec and DTMF payloads in RTP packets as described in RFC 2833 [17].

For cases where RFC 2833 [17] is not supported, the CND-SIP UA shall support transport of the DTMF tones inband in the RTP stream.

7.2.8 Capability Exchange

The CND-SIP UA should indicate its capabilities at registration, according to RFC 3840 [18]. The following feature tags may be indicated: sip.audio, sip.video, sip.text, sip.duplex, sip.mobility, sip.description, sip.events, sip.methods, sip.extensions, and sip.schemes.

When receiving a registration request from the CND-SIP UA, the CNG-SIP B2BUA should use the capability information contained in this request, to update a repository of the CND-SIP UAs capabilities. This repository may be used internally by the CNG-SIP B2BUA for its operation.

The CNG-SIP B2BUA may additionally poll the registered CND-SIP UAs using the SIP OPTIONS request, as specified in RFC 3261 [4], clause 11. The information received by the CND-SIP UA in the SIP OPTIONS response may be used by the CNG-SIP B2BUA for updating the information in the repository containing the CND-SIP UAs capabilities.

When receiving a SIP OPTIONS request the CND-SIP UA should generate a response according to RFC 3261 [4], clause 11.

7.3 Procedures for IMS devices

The Gm' supports non-IMS and IMS devices.

Non-IMS devices should comply with the procedures specified in clause 7.2.

IMS devices should comply with the procedures specified for the Gm reference point, with the exception that security associations are not supported when attaching to the NGN through the Gm' reference point.

7.3.1 Registration of a CND-IMS UA, using an IMS identity

The IMS CND should follow the procedures specified in ES 283 003 [5] in the following clauses:

- 5.1.1.2A
- 5.1.1.3
- 5.1.1.4A

The CNG-SIP Proxy B2BUA should forward all registration requests to the NGN in a transparent fashion. In parallel the CNG-SIP Proxy B2BUA may create a local registration entry for the CND-SIP UA in order to enable local services for the CND-SIP UA.

7.3.2 Registration of a CND-IMS UA, using a local identity

The IMS CND should follow the procedures specified in ES 283 003 [5] in the following clauses:

- 5.1.1.2A
- 5.1.1.3
- 5.1.1.4A

With the exception that a public user identity and the domain name valid in the NGN should not be used when populating the SIP header fields. Instead a local user identity and a local registration domain should be used. The local user identity contains a value that is administered by the CNG-SIP Proxy B2BUA and the value of the registration domain should be the registration domain handled by the CNG-SIP Proxy B2BUA.

7.3.3 Generic procedures for the CND-IMS UA and the CNG-SIP Proxy B2BUA for Basic Call and Conversational Supplementary Services

The CND-IMS UA within the CPN shall comply to the procedures specified for a UE, with the exception that procedures related to encrypted signalling and AKA authentication shall not be used for the Gm' reference point.

If the CNG-SIP Proxy B2BUA is implementing the CNG-SIP Proxy, it shall forward the SIP messages in a transparent fashion complying with the specification in clause 16 of RFC 3261 [4]. The role of a SIP ALG should be implemented in the proxy; i.e. while performing the routing of SIP messages, the CPN references should be interchanged to NGN references (and vice versa) for applicable header and body parts.

If implementing the CNG-SIP B2BUA, it shall comply to procedures specified for a UE on the CPN side, with the exception that procedures related to encrypted signalling and AKA authentication shall not be used for the Gm' reference point. On the NGN side the CNG-SIP B2BUA shall comply with the procedures specified for the Gm reference point, including the possible support for encryption and AKA authentication. A CNG-SIP B2BUA is implementing the role of SIP ALG.

The CNG-SIP B2BUA shall generate SIP messages in a transparent fashion, i.e. when receiving a SIP message on the CPN/NGN side the same request/response shall be generated on the other side, complying with the following generic rules:

- replacing applicable URI's to reference the correct side of the CNG-SIP B2BUA (depending on level of UE emulation for the CNG-SIP B2BUA, and the level of recommendation implemented for the ES 283 003 [5] and TS 183 028 [51] specifications);
- replacing applicable SDP parts of the SIP messages to reference the correct side of the CNG-SIP B2BUA;
- manage setup, modification and termination of media forwarding to support media negotiation when performed by the CND-IMS UA;
- forking should be supported on the CPN side when more than one local SIP-URI is associated with a public SIP-URI and/or when multiple contacts are registered for the same local-SIP URI.

7.3.4 Basic Call

The CND-IMS UA and the CNG-SIP B2BUA shall apply the generic procedures specified in clause 7.3.3 in combination with the procedures for a UE specified in TS 283 003 [5] and TS 183 028 [51].

The CNG-SIP Proxy shall apply the generic procedures specified in clause 7.3.3.

7.3.5 Conversational Supplementary Services

7.3.5.1 Activation/deactivation of services

NOTE: Activation/deactivation of services is not elaborated in Release 2.

7.3.5.2 Communication Diversion

When Communication Diversion is supported, the CND-IMS UA and the CNG-SIP B2BUA shall apply the generic procedures specified in clause 7.3.3 in combination with the procedures for a UE specified in TS 183 004 [52].

When Communication Diversion is supported, the CNG-SIP Proxy shall apply the generic procedures specified in clause 7.3.3.

7.3.5.3 Communication Rejection

When Communication Rejection is supported, the CND-IMS UA and the CNG-SIP B2BUA shall apply the generic procedures specified in clause 7.3.3 in combination with the procedures for a UE specified in TS 183 011 [53].

When Communication Rejection is supported, the CNG-SIP Proxy shall apply the generic procedures specified in clause 7.3.3.

7.3.5.4 Explicit Communication Transfer

When Explicit Communication Transfer is supported, the CND-IMS UA and the CNG-SIP B2BUA shall apply the generic procedures specified in clause 7.3.3 in combination with the procedures for a UE specified in TS 183 029 [54].

When Explicit Communication Transfer is supported, the CNG-SIP Proxy shall apply the generic procedures specified in clause 7.3.3.

7.3.5.5 Communication Hold

When Communication Hold is supported, the CND-IMS UA and the CNG-SIP B2BUA shall apply the generic procedures specified in clause 7.3.3 in combination with the procedures for a UE specified in TS 183 010 [55].

When Communication Hold is supported, the CNG-SIP Proxy shall apply the generic procedures specified in clause 7.3.3.

7.3.5.6 Conference (3-Party)

When Conference (3-Party) is supported, the CND-IMS UA and the CNG-SIP B2BUA shall apply the generic procedures specified in clause 7.3.3 in combination with the procedures for a UE specified in TS 183 005 [34].

When Conference (3-Party) is supported, the CNG-SIP Proxy shall apply the generic procedures specified in clause 7.3.3.

7.3.5.7 Message Waiting Indication

When Message Waiting Indication is supported, the CND-IMS UA and the CNG-SIP B2BUA shall apply the generic procedures specified in clause 7.3.3 in combination with the procedures for a UE specified in TS 183 006 [15].

When Message Waiting Indication is supported, the CNG-SIP Proxy shall apply the generic procedures specified in clause 7.3.3.

7.3.5.8 Originating Identification

When Originating Identification is supported, the CND-IMS UA and the CNG-SIP B2BUA shall apply the generic procedures specified in clause 7.3.3 in combination with the procedures for a UE specified in TS 183 007 [43].

When Originating Identification is supported, the CNG-SIP Proxy shall apply the generic procedures specified in clause 7.3.3.

7.3.5.9 Terminating Identification

When Terminating Identification is supported, the CND-IMS UA and the CNG-SIP B2BUA shall apply the generic procedures specified in clause 7.3.3 in combination with the procedures for a UE specified in TS 183 008 [36].

When Terminating Identification is supported, the CNG-SIP Proxy shall apply the generic procedures specified in clause 7.3.3.

7.3.5.10 Malicious Communication Identification

When Malicious Communication Identification is supported, the CND-IMS UA and the CNG-SIP B2BUA shall apply the generic procedures specified in clause 7.3.3 in combination with the procedures for a UE specified in TS 183 016 [35].

When Malicious Communication Identification is supported, the CNG-SIP Proxy shall apply the generic procedures specified in clause 7.3.3.

7.3.5.11 Advice of Charge

When Advice of Charge is supported, the CND-IMS UA and the CNG-SIP B2BUA shall apply the generic procedures specified in clause 7.3.3 in combination with the procedures for a UE specified in TS 183 047 [40].

When Advice of Charge is supported, the CNG-SIP Proxy shall apply the generic procedures specified in clause 7.3.3.

7.3.5.12 Closed User Groups

When Closed User Groups is supported, the CND-IMS UA and the CNG-SIP B2BUA shall apply the generic procedures specified in clause 7.3.3 in combination with the procedures for a UE specified in TS 183 054 [41].

When Closed User Groups is supported, the CNG-SIP Proxy shall apply the generic procedures specified in clause 7.3.3.

7.3.5.13 DTMF

When DTMF is supported, the CND-IMS UA and the CNG-SIP B2BUA shall apply the generic procedures specified in clause 7.3.3 in combination with the procedures specified for DTMF signalling for a UE in TS 124.229 [20].

When DTMF is supported, the CNG-SIP Proxy shall apply the generic procedures specified in clause 7.3.3.

7.3.5.14 User Capabilities

When Capability Exchange is supported, the CND-IMS UA shall apply the procedures endorsed by ES 283 003 [5] related to RFC 3840 [18] implementation and usage of the SIP OPTIONS request.

Upon receiving a registration request from a CND-IMS UA that contains capability information, the CNG-SIP B2BUA should use this information to update a local repository containing the CND-IMS UAs capabilities. This repository may be used by the CNG-SIP B2BUA for its operation.

The CNG-SIP B2BUA may additionally poll the registered CND-IMS UAs using the SIP OPTIONS request, as specified in RFC 3261 [4], clause 11. The information received by the CND-IMS UA in the SIP OPTIONS response may be used by the CNG-SIP B2BUA for updating the information in the repository containing the CND-IMS UAs capabilities.

7.3.6 Presence

When Presence is supported, the CND-IMS UA and the CNG-SIP B2BUA shall apply the generic procedures specified in clause 7.3.3 in combination with the procedures specified for a UE in ES 283 030 [16].

Where Presence is supported, the CNG-SIP Proxy shall apply the generic procedures specified in clause 7.3.3.

7.3.7 Messaging

When Messaging is supported, the CND-IMS UA and the CNG-SIP B2BUA shall apply the generic procedures specified in clause 7.3.3 in combination with the procedures specified for a UE in TS 183 041 [33].

When Messaging is supported, the CNG-SIP Proxy shall apply the generic procedures specified in clause 7.3.3.

7.3.8 SMS/MMS

When SMS/MMS is supported, the CND-IMS UA and the CNG-SIP B2BUA shall apply generic procedures specified in clause 7.3.3 in combination with the procedures specified for a UE in TS 183 051 [42].

When SMS/MMS is supported, the CNG-SIP Proxy shall apply the generic procedures specified in clause 7.3.3.

7.4 Procedures for NAT traversal

If the CNG-SIP Proxy B2BUA implements a SIP Proxy, the SIP Proxy should implement SIP ALG functionality. The SIP ALG functionality assists the SIP based applications in the CND with NAT traversal.

If the CNG-SIP Proxy B2BUA implements a SIP B2BUA, the SIP B2BIA shall implement SIP ALG functionality for the SIP based applications using the Gm' reference point.

The CNG-SIP Proxy B2BUA may perform relevant modifications of the SIP messages headers and body sections in order to handle the NAT functionality performed internally by the CNG.

Furthermore, by using the internal interface towards to CNG-NAPT and Firewall Function, the CNG-SIP Proxy B2BUA initiates and terminates port forwarding needed by the sessions. This is done on a per-session basis.

The CNG NAT traversal may be performed using the P-CSCF functionalities described in TS 123 228 [61], annex G and RACS specified in clause 6.3.3.1.1 in ES 282 003 [60].

7.5 CNG-SIP Proxy B2BUA Operation

In the architecture specified by TS 185 003 "TISPAN CNG Architecture and Reference Points" [1] Gm' is the reference point between CND-SIP UA and CNG-SIP Proxy B2BUA. In the same document a definition is made of the CNG-SIP Proxy B2BUA Function.

This functionality may be implemented either as a SIP Proxy as specified in RFC 3261 [4] or a SIP B2BUA as defined in RFC 3261 [4], in either case extended with the necessary extension in order to be able to attach to the P-CSCF by usage of the Gm reference point.

The "SIP Proxy" is specified in RFC 3261 [4], both regarding to protocol handling and regarding the routing functionality to be performed. If implementing a SIP proxy in the CNG, network topology information will not be hidden between the CPN and NGN sides. A SIP Proxy can not initiate its own sessions and in most cases it does not initiate its own transactions. The functionality of a SIP Proxy is specified as being that of a rather transparent SIP router.

Since a "SIP Proxy" in general does not initiate own signalling it is not suitable for a protocol adaptation functionality between IETF SIP and IMS SIP. It could be used in the path for communication from "early IMS CND" to the NGN. This would allow ALG functionality, local services, QoS functionality and Admission Control performed by the CNG. In case a "SIP Proxy" would be used from non-IMS SIP CND, the IMS protocol adaptation would have to be made by the NGN and the signalling between the CNG-SIP Proxy and the NGN P-CSCF would not comply with the specification of the Gm reference point.

A "SIP B2BUA" is following the specification of a SIP UA in RFC 3261 [4]. Regarding to protocol handling it conforms to the specification of a SIP UA. Regarding the functionality of a B2BUA it is completely implementation dependant and not specified by the RFC 3261 [4]. This means in general a SIP B2BUA could implement routing functionality in a proxy-like fashion, or it could implement other functionality (for further studies). A SIP B2BUA terminates sessions on one side and initiates sessions on the other side by applying specific logic that the B2BUA implements. If implementing a B2BUA in the CNG, network topology information would be hidden between the CPN and NGN sides of the CNG.

Since a "SIP B2BUA" initiates and terminates sessions it will be suitable both for IETF SIP <-> IMS SIP protocol adaptations as well as ALG functionality, enabling local services, QoS, and local admission control.

8 Procedures at the e3' reference point

8.1 General

A CND may support the e3 reference point for direct remote management from the CNGCF, as specified in TS 183 065 [21]. The e3 reference point provides a complete set of management functionalities (e.g. provisioning and configuration management, software/firmware management, diagnostics and troubleshooting, performance monitoring).

In addition or as an alternative, some management functionalities (e.g. provisioning) may be provided by means of the e3' reference point.

8.2 Procedures for using HTTP

8.2.1 Data model definition

As specified in TS 183 065 [21], the CND data model shall be compliant with the data models already defined by Broadband Forum in its technical reports, e.g.:

- TR-106 Amendment 2 [63], generic TR-069 [89] device data model;
- TR-104 [62], VoIP device data model;
- TR-135 [64], IPTV STB data model;
- TR-140 Issue 1.1 [65], Storage device data model.

8.2.2 Configuration and provisioning

As specified in TS 183 065 [21], configuration management and provisioning may be done through the e3 reference point.

In addition, the basic provisioning of the CND may be achieved by means of the e3' protocol specified in clause 8.2.2.1: in general such a solution may be used when the CND does not support the e3 reference point or when it is better suited for a simple provisioning of configuration data that are pre-provisioned on the CNG.

To summarize: a CND may be provisioned by using the e3 reference point, the e3' reference point or manually.

- If the CNG supports the e3' protocol, a CND supporting e3' protocol will be successfully provisioned by the CNG.
- If the CNG does not support the e3' protocol, a CND not supporting e3' protocol may be provisioned only with e3 protocol by the CNGCF or manually by the end-user.

In case a CND supports both e3 and e3', then, in order to choose a reference point between e3 and e3', it is necessary to distinguish two cases:

- Case 1: Configuration parameters are provisioned by CNGCF to CND indirectly (trough the CNG: e3'reference point).
- Case 2: Configuration parameters are provisioned by CNGCF to CND directly (e3 reference point).

The CND's behaviour shall be the following:

- the CND sends the configuration request message, on e3', to the CNG;
- if the CNG answers with the list of configuration parameters, then Case 1 is followed;
- if the CND gets an error or the CNG answers with an error message, then Case 2 is followed and the CND can therefore send a notification (by means of the Inform RPC), on e3 (CWMP), to the CNGCF in order to request the necessary configuration data (it is up to the CNGCF to provision the appropriate configuration data to the managed CNDs).

In the remaining of the clause a CND Configuration Protocol on the e3'reference point, for the provisioning of identities for accessing the NGN services, is proposed.

NOTE: The CND Configuration Protocol on e3' does not implement any mechanism to protect the information flow for TISPAN Release 2.

8.2.2.1 CND Configuration Protocol (on the e3' reference point)

The CND Configuration Protocol (CNDCP) on the e3' reference point may be used when a CND is not provided with the necessary configuration data to access the NGN services (i.e. SIP username and password, SIP domain, SIP outbound proxy), but instead the CNG has already been provisioned with all of these configuration data: through CNDCP, a CND may automatically acquire the necessary configuration data from the CNG and then access the NGN services, with no need of other configuration tasks. Indeed, appropriate commands may be provided to the end-user on the CND User Interface for triggering the CNDCP messages: this allows the end-user to reconfigure the CND with simple selections of menu entries in the CND User Interface.

This version of the CNDCP protocol is suited for the configuration of SIP CND compliant to RFC 3261 [4].

A use case for the CNDCP protocol is the following:

- the CNG is pre-provisioned with a list of available SIP identities, and other corresponding SIP parameters, for accessing the NGN services from the Customer Network;
- a new CND with no SIP identity configured may request and select a SIP identity by means of CNDCP: this may be an automatic request of the CND at its bootstrap, so that the CND is able to access the NGN services without any user intervention;

- in any case, the CND user may manually change the SIP identity assigned to the CND, e.g. by means of appropriate CND User Interface menu items for triggering the corresponding CNDCP commands.

The CNDCP protocol may be used not only in the first phase of provisioning and configuration of the CND, but also when the customer wants to change the associated CLI (Customer Line Identifier) to his own CND using a different SIP identity from the one previously configured. Even if the CNG always sends the whole set of SIP parameters in each CNDCP answer, the CND may select which SIP identity to use.

The CNDCP protocol is based on HTTP protocol: the CND requests are sent through an HTTP GET to the CNG, which will reply with XML messages containing configuration data and/or error notice.

The details of the CNDCP protocol and the structure of the XML messages used are described in the following clauses.

In details, through CNDCP protocol the CNG provides the CND (in the role of SIP end-point) with the following SIP configuration parameters, which should be pre-provisioned on the CNG (e.g. on the e3 reference point, using TR-069 [90] remote management):

- the **SIP Username**, i.e. the IMPU (SIP-URI or TEL-URI) used for accessing the NGN services; in the remaining of the clause this parameter is also referenced as CLI;

  (in case the CNG is provisioning on the e3 reference point, the corresponding TR-104 [62] parameter is: InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.DirectoryNumber);

- the **SIP Password** (or SIP Key) for authenticating the access to the NGN services;

  (in case the CNG is provisioning on the e3 reference point, the corresponding TR-104 [62] parameter is: InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.Line.{i}.SIP.AuthPassword);

- the **SIP Domain** for the SIP Username;

  (in case the CNG is provisioning on the e3 reference point, the corresponding TR-104 [62] parameter is: InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.UserAgentDomain);

- the IP address of the **SIP Outbound Proxy;**

  (in case the CNG is provisioning on the e3 reference point, the corresponding TR-104 [62] parameter is: InternetGatewayDevice.Services.VoiceService.{i}.VoiceProfile.{i}.SIP.OutboundProxy).

8.2.2.1.1 Protocol Description

The CNDCP protocol is based on HTTP: the CNG shall behave as HTTP server and the CND as HTTP client. The CND requests are sent in the form of a HTTP GET to a specific URL sent to the address of current Default Gateway and the CNG answers with an XML message containing an error code (code 0 indicates the correct request) and the configuration parameters.

The CND shall be able to send three types of HTTP GET requests to the CNG, as in the following URLs:

1) http://<<IP_default_gateway>>/AskCli

2) http://<<IP_default_gateway>>/GetCliInfo?CLI=<<first_CLI>>&CLI=<<second_CLI>>&CLI=<<third_CLI>>&CLI=<<fourth_CLI>>&CLI=<<fifth_CLI>>&.....CLI=<<nth_CLI>>

3) http://<<IP_default_gateway>>/DelAllCli

where:

- <<IP_default_gateway>> is the IP address of the default gateway;

- <<n_CLI>> is the SIP Username, and is an alphanumerical string of maximum 32 characters.

The URL #1 (AskCli) shall be requested by the CND to retrieve the complete list of available CLIs that can be assigned to the CNDs. This URL is used at the first provisioning of the CND. CNG will answer with an XML file including the list of both the available and already used CLIs; for each CLI in the list, the CNG may also indicate the host name of CND that is currently using the CLI.

The URL #2 (GetCliInfo) shall be used by the CND to request the CNG to reserve the specified CLI of the list of specified CLIs for its usage (in the case that the CND can manage more than one CLI). The CNG will answer with a XML file including the configuration data to be used by SIP user agent on the CND. The URL #2 shall be used also in the cases where the CND must re-confirm the association with its CLIs, e.g. in the following cases:

- at each boot of an already configured CND (i.e. already associated to a CLI);
- when a Wi-Fi CND is re-entering under radio coverage;
- following the reception of a specific message from the CNG (message of request of configuration renewal, see clause 8.2.2.1.4);
- at the DHCP lease time expiration;
- in order to remove the association of one or more CLIs (in such cases, the CND shall reconfirm only the ones still used).

As an example, if two CLIs can be managed by the CND (CLI=0123456789 and 2345678901), the following URL must be requested:

- http://192.168.1.1/GetCliInfo&CLI=0123456789&CLI=2345678901.

When a CND requests the release of associated CLIs, the CND shall request the URL #2 or the URL #3, depending on the number of CLIs used by the CND.

If the request is to delete one CLI but the other CLIs remain associated, the CND shall use URL #2, where the CLI to be deleted is not present. For example, if three CLIs are configured in the CND (CLI=0123456789, 2345678901 and 3456789012) and the user requests to release the 0123456789, the following URL must be requested by the CND:

- http://192.168.1.1/GetCliInfo&CLI=2345678901&CLI=3456789012.

The previous command confirms the association with the CLIs already associated.

If the request is to delete the ONLY CLI still associate or to release all CLIs associated to the CND, the CND shall use URL #3 (DelAllCli). As an example, if the CND releases the CLI=0123456789 and this is the last CLI associated to the CND, the CND must request the following URL:

- http://192.168.1.1/DelAllCli.

The XML schema for the answer messages sent by CNG is described in figure 8.1.

```
<?xml version="1.0"?>
<xs:schema targetNamespace="http://uri.etsi.org/ngn/customernetwork/xml/apt-config_version-1"
xmlns:aptcfg="http://uri.etsi.org/ngn/customernetwork/xml/apt-config_version-1"
xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified"
attributeFormDefault="qualified" id="NewDataSet">
   <xs:complexType name="ErrorStatusType">
      <xs:sequence>
         <xs:element name="ErrorCode" maxOccurs="unbounded">
            <xs:complexType>
               <xs:simpleContent>
                  <xs:extension base="xs:integer">
                     <xs:attribute name="CLI" type="xs:string" use="optional"/>
                  </xs:extension>
               </xs:simpleContent>
            </xs:complexType>
         </xs:element>
      </xs:sequence>
   </xs:complexType>
   <xs:complexType name="CLIListType">
      <xs:sequence>
         <xs:element name="CLI" maxOccurs="unbounded">
            <xs:complexType>
               <xs:simpleContent>
                  <xs:extension base="xs:string">
                     <xs:attribute name="Status" use="required">
                        <xs:simpleType>
                           <xs:restriction base="xs:string">
                              <xs:enumeration value="Available"/>
                              <xs:enumeration value="NotAvailable"/>
                              <xs:enumeration value="Registered"/>
```

```
                        </xs:restriction>
                     </xs:simpleType>
                  </xs:attribute>
                  <xs:attribute name="Host" type="xs:string" use="optional"/>
               </xs:extension>
            </xs:simpleContent>
         </xs:complexType>
      </xs:element>
   </xs:sequence>
</xs:complexType>
<xs:complexType name="SIPCNDParametersType">
   <xs:sequence>
      <xs:element name="OutboundProxyIP" type="xs:string"/>
      <xs:element name="LineIdentification" type="xs:string"/>
      <xs:element name="SIPkey" type="xs:string"/>
      <xs:element name="SIPDomain" type="xs:string" minOccurs="0"/>
   </xs:sequence>
</xs:complexType>
<xs:element name="APTData">
   <xs:complexType>
      <xs:sequence>
         <xs:element name="ErrorStatus" type="aptcfg:ErrorStatusType" minOccurs="0"
maxOccurs="unbounded"/>
         <xs:element name="CLIList" type="aptcfg:CLIListType" minOccurs="0"
maxOccurs="unbounded"/>
         <xs:element name="SIPCNDParameters" type="aptcfg:SIPCNDParametersType" minOccurs="0"
maxOccurs="unbounded"/>
      </xs:sequence>
   </xs:complexType>
</xs:element>
</xs:schema>
```

Figure 8.1 XML Schema for answer messages sent by the CNG

8.2.2.1.2 CLI-CND Association

For associating a CND to a CLI, usually the first step is to ask the CNG for the CLI list (automatically or by user interaction). The CLI list request is sent by means of the HTTP GET request with the following URL (URL #1):

- http://192.168.1.1/AskCli;

where it is assumed that the IP address of the default gateway is 192.168.1.1. The response consists in an XML message, containing the error code and the list of the CLI's (available and already used); the possibilities are listed in table 8.1.

Table 8.1

Result of procedure	Error Code	Description	XML Format	Example of user message
Correct	0	The CNG answers with an XML message with the list of the CLI's and the Status of each CLI (Registered or Available), and optionally the Host name for the already registered CLIs	Figure 8.2	Available CLI's List.
Not Available	1	No CLI available in the CNG because the network provisioning is not yet completed. The XML message sent by the CNG contains only the notification of the error with ErrorCode=1	Figure 8.3	Telephone number not available. Please retry later.

Following to the CLI list request, the user can request the association of one or more CLI to the CND, using the URL #2. The CNG answers by an XML message that reports the results of the association request (successful or not) for each CLI. Some examples for XML message sent by CNG for CLI association are available in clause8.2.2.1.5

Once that the association between a CLI and the CND IP address is created, the CNG will update it based on the DHCP mechanism. In detail, the CLI/CND association will expire when:

- the lease time DHCP expires and the CND does not renew the DHCP request. In this case the CLI association is released and the CLI is available for other CNDs;
- the CND is correctly turned off; for example, in this case, the CND will send the SIP REGISTER message (for de-registration, updating the SIP presence information on the network) and the DHCP RELEASE (RFC 2131 [23]) message towards its own DHCP server (CNG). Upon receiving the DHCP RELEASE, the CNG shall update its own DHCP server IP table and delete associations between the released IP address and CLIs. All the CLIs assigned to a CND that sends a DHCPRELEASE message then become available for other CNDs;
- the CND sends out a new multiple registration where one or more CLI's, previously associated to it, are no longer present in the requested URL;
- the CND receives a request for CCRP (see clause 8.2.2.1.4) from the CNG: the CCRP activation may happen when the CNG turns on after a loss of power or a modification of PPPoE session public IP address or the VoIP parameters are pre-provisioned by the CNGCF. Through the CCRP, the CND renews the association by means of an HTTP GET request, whose URL contains all the CLI's that were previously associated to that CND. More details on this procedure are available in clause 8.2.2.1.4;
- the CND carries out the removal request of the CLI association.

8.2.2.1.3 Removing CLI Association

A CND can request the CNG to remove a CLI association. If the CND is using multiple CLI, the CLI de-association request is carried on through an association request URL (URL #2) where the CLI to be removed is not present.

For example if CLI1=0612345678 and CLI2=0698765432 are associated to a CND that sends the following request:

- http://192.168.1.1/GetCliInfo&CLI=0612345678.

The above request must be considered by the CNG as a request to remove the association with CLI2: the CLI2 must be released and it is available for other CNDs. If the CND uses a single CLI and requests to remove this association, it must be sent to the CNG the request to delete all CLI association, using the URL # 3.

8.2.2.1.4 Compulsory Configuration Renewal

It is required that the CNG is able to force the CNDs to request the configuration parameters by sending a specific IP/UDP message in broadcast to the LAN MAC addresses.

The Compulsory Configuration Renewal Procedure (CCRP) is activated by the CNG in the following situations:

- at each start-up of the CNG;
- in case of re-connection and assignment of the new public IP address to the WAN interface for the PPPoE management session. The CCRP must not start in case of a first PPPoE session establishment after CNG start-up, but only after a disconnect/re-connect of PPPoE session; the purpose is to update the NAPT table in case of new IP address assignment on WAN interface.

To activate CCRP, CNG sends on all of its LAN interfaces a 64 bytes length IP packet, formatted as following:

- Eth MAC source address: CNG LAN Interface MAC address
- Eth MAC destination address: broadcast
- IP source address: LAN default gateway (CNG LAN interface IP address)
- IP destination address: 255.255.255.255
- Protocol: UDP
- UDP source port: 50062

- UDP destination port: 50062
- UDP payload: the following 36 bytes in HEX:
  - xx xx 55 41 49 50 41 49 50 4f 4e 55 41 49 50 41
  - 49 50 4f 4e 55 41 49 50 41 49 50 4f 4e 55 41 49
  - 50 41 49 50

where xx xx represents UDP payload identification number (different values in different packets).

When the CCRP starts, the CNG sends for 5 times and each 15 s a group of messages with the same UDP payload identification number; the next event that will cause a new CCRP will have a different UDP payload identification number (for example, randomly generated). The CND will react only to the first group of UDP messages received with the same UDP payload identification number.

8.2.2.1.5 Example of XML File

8.2.2.1.5.1 CLI LIST XML FILE

Figure 8.2 shows an example of XML file sent from the CNG to the CND in the case of request for CLI List. 7 CLI are provisioned in the CNG (0112285111, 0112285112, 0112285113, 0112285114, 0112285115, 0112285116, 0112285117) and 5 of these CLIs are already associated to other CNDs (Status=Registered). The CND can only select one of the two available numbers (Status=Available).

```
<?xml version="1.0" encoding="UTF-8"?>
<aptcfg:APTData xmlns:aptcfg="http://uri.etsi.org/ngn/customernetwork/xml/apt-config_version-1"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <aptcfg:CLIList>
      <aptcfg:CLI aptcfg:Status="Registered" aptcfg:Host ="host1">0112285111</aptcfg:CLI>
      <aptcfg:CLI aptcfg:Status="Registered" aptcfg:Host ="host2">0112285112</aptcfg:CLI>
      <aptcfg:CLI aptcfg:Status="Registered" aptcfg:Host ="host3">0112285113</aptcfg:CLI>
      <aptcfg:CLI aptcfg:Status="Available">0112285114</aptcfg:CLI>
      <aptcfg:CLI aptcfg:Status="Available">0112285115</aptcfg:CLI>
      <aptcfg:CLI aptcfg:Status="Registered" aptcfg:Host ="host4">0112285116</aptcfg:CLI>
      <aptcfg:CLI aptcfg:Status="Registered" aptcfg:Host ="host5">0112285117</aptcfg:CLI>
   </aptcfg:CLIList>
</aptcfg:APTData>
```

Figure 8.2: XML File for visualization available CLI

When the CND receives the XML file as in figure 8.2, the CND User Interface may show to the customer the CLI list, marking the CLI already registered. When the customer selects an available CLI, the CND sends an HTTP GET for requesting the CLI association.

If the CNG has no SIP parameters, because the provisioning is not complete, the following XML file must be sent:

```
<aptcfg:APTData xmlns:aptcfg="http://uri.etsi.org/ngn/customernetwork/xml/apt-config_version-1"
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <aptcfg:ErrorStatus>
      <aptcfg:ErrorCode>1</aptcfg:ErrorCode>
   </aptcfg:ErrorStatus>
</aptcfg:APTData>
```

Figure 8.3: XML File for provisioning data lack

8.2.2.1.5.2 CLI Association XML File

In figures 8.4 to 8.9, some examples of XML files for CLI association are reported.

```
<?xml version="1.0" encoding="UTF-8"?>
<aptcfg:APTData xmlns:aptcfg="http://uri.etsi.org/ngn/customernetwork/xml/apt-config_version-1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <aptcfg:ErrorStatus>
      <aptcfg:ErrorCode aptcfg:CLI="0112285114">0</aptcfg:ErrorCode>
   </aptcfg:ErrorStatus>
   <aptcfg:SIPCNDParameters>
      <aptcfg:OutboundProxyIP>80.92.181.1</aptcfg:OutboundProxyIP>
      <aptcfg:LineIdentification>0112285114</aptcfg:LineIdentification>
      <aptcfg:SIPkey>10af03940aaef</aptcfg:SIPkey>
      <aptcfg:SIPDomain>example.com</aptcfg:SIPDomain>
   </aptcfg:SIPCNDParameters>
</aptcfg:APTData>
```

Figure 8.4: "Error code 0" - Configuration procedure successful - single CLI requested and associated

```
<?xml version="1.0" encoding="UTF-8"?>
<aptcfg:APTData xmlns:aptcfg="http://uri.etsi.org/ngn/customernetwork/xml/apt-config_version-1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <aptcfg:ErrorStatus>
      <aptcfg:ErrorCode aptcfg:CLI="0112285114">0</aptcfg:ErrorCode>
      <aptcfg:ErrorCode aptcfg:CLI="0112285115">0</aptcfg:ErrorCode>
   </aptcfg:ErrorStatus>
   <aptcfg:SIPCNDParameters>
      <aptcfg:OutboundProxyIP>80.92.181.1</aptcfg:OutboundProxyIP>
      <aptcfg:LineIdentification>0112285114</aptcfg:LineIdentification>
      <aptcfg:SIPkey>10af03940aaef</aptcfg:SIPkey>
      <aptcfg:SIPDomain>example.com</aptcfg:SIPDomain>
   </aptcfg:SIPCNDParameters>
   <aptcfg:SIPCNDParameters>
      <aptcfg:OutboundProxyIP>80.92.181.1</aptcfg:OutboundProxyIP>
      <aptcfg:LineIdentification>0112285115</aptcfg:LineIdentification>
      <aptcfg:SIPkey>003edafe34bcb</aptcfg:SIPkey>
      <aptcfg:SIPDomain>example.com</aptcfg:SIPDomain>
   </aptcfg:SIPCNDParameters>
</aptcfg:APTData>
```

Figure 8.5: "Error code 0" - Configuration procedure successful - two-CLI requested and associated

```
<aptcfg:APTData xmlns:aptcfg="http://uri.etsi.org/ngn/customernetwork/xml/apt-config_version-1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <aptcfg:ErrorStatus>
      <aptcfg:ErrorCode aptcfg:CLI="0112285114">1</aptcfg:ErrorCode>
   </aptcfg:ErrorStatus>
</aptcfg:APTData>
```

Figure 8.6: "Error code 1" - Unsuccessful configuration procedure due to lack of provisioning data In this case no VoIP parameters are configured in the CNG

```
<aptcfg:APTData xmlns:aptcfg="http://uri.etsi.org/ngn/customernetwork/xml/apt-config_version-1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <aptcfg:ErrorStatus>
      <aptcfg:ErrorCode aptcfg:CLI="0112285114">1</aptcfg:ErrorCode>
      <aptcfg:ErrorCode aptcfg:CLI="0112285115">0</aptcfg:ErrorCode>
   </aptcfg:ErrorStatus>
   <aptcfg:SIPCNDParameters>
      <aptcfg:OutboundProxyIP>80.92.181.1</aptcfg:OutboundProxyIP>
      <aptcfg:LineIdentification>0112285115</aptcfg:LineIdentification>
      <aptcfg:SIPkey>003edafe34bcb</aptcfg:SIPkey>
      <aptcfg:SIPDomain>example.com</aptcfg:SIPDomain>
   </aptcfg:SIPCNDParameters>
</aptcfg:APTData>
```

Figure 8.7: "Error code 1" - Unsuccessful configuration procedure due to lack of provisioning data for first CLI and correct data for second CLI

```
<aptcfg:APTData xmlns:aptcfg="http://uri.etsi.org/ngn/customernetwork/xml/apt-config_version-1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <aptcfg:ErrorStatus>
      <aptcfg:ErrorCode aptcfg:CLI="0112285114">2</aptcfg:ErrorCode>
   </aptcfg:ErrorStatus>
</aptcfg:APTData>
```

Figure 8.8: "Error code 2" - Unsuccessful configuration procedure due to wrong typed CLI

```
<aptcfg:APTData xmlns:aptcfg="http://uri.etsi.org/ngn/customernetwork/xml/apt-config_version-1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<aptcfg:ErrorStatus>
<aptcfg:ErrorCode aptcfg:CLI="0112285114">3</aptcfg:ErrorCode>
</aptcfg:ErrorStatus>
</aptcfg:APTData>
```

Figure 8.9: "Error code 3" - Unsuccessful configuration procedure due to CLI already allocated

For each error code the CND that has requested the CLI could show an appropriate message for the user, in the CND User Interface.

8.2.3 Software management

As specified in TS 183 065 [21], software management may be done through the e3 reference point.

8.2.4 Diagnostics

As specified in TS 183 065 [21], diagnostics may be done through the e3 reference point.

8.2.5 Performance Monitoring

As specified in TS 183 065 [21], performance monitoring may be done through the e3 reference point.

9 Procedures at the au Reference Point

9.1 General

The au reference point is defined between the Customer Network Device and the CNG-AuF.

The authenticated entity is a CND (Customer Network Device), while the authenticator is the CNG (Customer Network Gateway) as specified by TS 185 003 [1].

9.2 Procedures for pairing CND-CNG

9.2.1 Identification of CNG

A CNG should support multiple SSIDs.

This will make it possible to setup a separate SSID with separate pairing and security.

Separate authentication should be used for each SSID.

9.2.2 Protocols on the au Reference Point

NOTE: The following normative text applies mainly to the wireless CNDs but can be theoretically valid for every possible CND.

The au reference point shall support WPA2 [30] as the secure protocol. In the case where the CND does not support WPA2 then WPA shall be supported as a fallback solution.

WPA/WPA2 is specified by Wi-Fi alliance and the specification is based of the standard IEEE 802.11i [31].

IEEE 802.1x [28] and EAP [29] are used in the WPA/WPA2 specification. WPA2 is using AES as security mechanism.

Overview scenario for mutual local authentication for WPA/WPA2 is shown on figure 9.1.

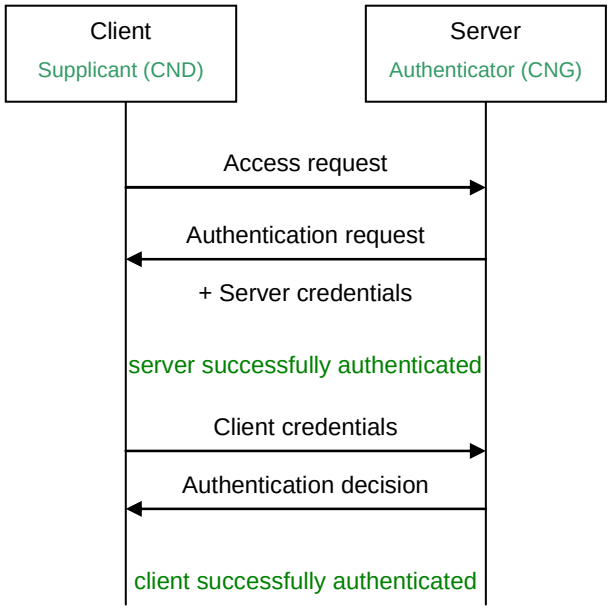


Figure 9.1: Mutual authentication scenario

The first couple of messages allow the server to be authenticated by the client, while the second pair is allowing the supplicant authentication.

In the case of au reference point usage the CND acts as Supplicant while the CNG, acting as wireless Access Point, is the Authenticator (there is no involvement of any network server).

9.2.2.1 Local authentication protocol

The base authentication protocol is EAP [29].

The protocol stack for a Supplicant and Authenticator conversation is shown on figure 9.2. The lower layer with respect to EAP which is used is IEEE 802.1X [28] and IEEE 802.11 [31]. The EAP method layer implements authentication algorithm, sends and receives EAP messages and handles fragmentation if needed.

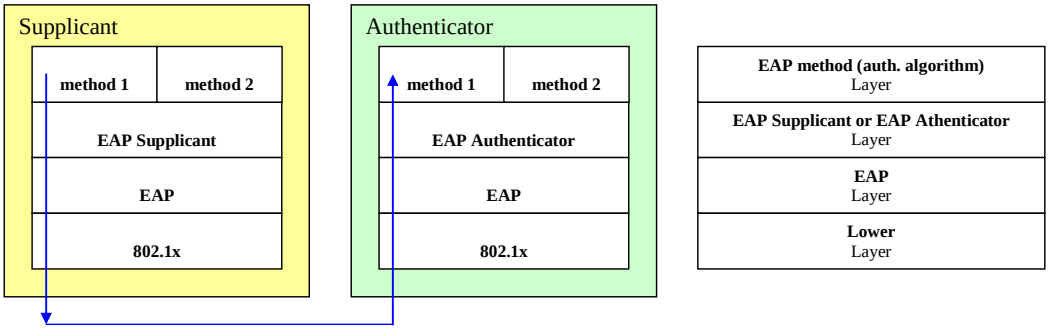


Figure 9.2: EAP entities layers

CNG is an Access Point (AP, IEEE 802.1X [28] authenticator) and Access Controller (AC), granting access to the residential network based on an access list of authorized users.

- Authentication protocol: IEEE 802.1X [28] (EAP) (WPA (Wi-Fi Protected Access)).

9.2.3 Simplified device pairing, Wi-Fi protected setup

The CNG and the CND shall support Wi-Fi Protected Setup Specification [32] as specified by Wi-Fi alliance.

This standard provides a secure way to configure WPA/WPA2 without the need for the user to enter a pass phrase into the AP. The user friendly mechanism shall support Wi-Fi Alliance Protected SetupTM (PIN/PBC).

The WPA/WPA2 pre-shared key provisioned by the user friendly mechanism should be at least eight characters, pseudo-random and consisting of digits 0 to 9 and characters a to z.

10 Procedures at the e1' Reference Point

10.1 Procedures for using DHCP

The e1' reference point serves the CND-AtF with appropriate configuration data to connect to a local IP network and attach to some selected services such as the P-CSCF. The protocol of choice is DHCP (RFC 2131 [23]) and the following clauses describes which DHCP options are needed to implement this function.

10.1a Procedures for using DHCP

The CNG-Attachment Function (CNG-AtF) should provide network attachment functionality as transparent as possible in order to be non-intrusive towards CNDs.

A DHCP server shall be contained within the CNG-AtF in the CNG to provide local IP addresses for the CNDs within the CPN.

A CND-AtF shall implement functionality as described in TS 183 019 [24], clause 7.1.1. For IPv6, the UE procedures specified in TS 183 019 [24] clause 7.2 shall be implemented.

A CNG-AtF shall implement the procedures specified in TS 183 019 [24], clause 7.1.3.

The IP addresses offered to CNDs should be selected in a random fashion to avoid address collisions when connecting home networks through IP tunnels.

10.2 Provisioning of DHCP server response parameters in the CNG

For cases when the CNG needs to provide parameters through DHCP options to the CNDs that are unknown at manufacturing time of the CNG, it should be possible to provision the CNG with this information.

One of the methods specified in the following clauses should then be supported.

10.2.1 TR-069 provisioned DHCP parameters

If the CNG implements the CWMP protocol specified in TR-069 amendment 2 [25], it should implement the DHCP server provisioning data model as defined in TR-098 amendment 2 [26]. This allows the operator to configure the correct DHCP option response values for the CNDs as defined in TS 183 019 [24], clause 7.1.1 or for IPv6 as defined in TS 183 019 [24], the UE parts of clause 7.2.

10.2.2 DHCP INFORM to obtain parameters

If the DHCP server response parameters in the CNG can not be provisioned according to 10.2.1 the CNG should implement a DHCP INFORM function for any unknown device requesting configuration. In this case the CNG may not have the knowledge about the device that has identified itself by the DHCP option 125 and instead of just ignoring the requested parameters per DHCP option 55 the CNG should send an outbound DHCPINFORM request to the WAN DHCP server to obtain these. DHCPINFORM is defined by RFC 2131 [23].

10.2.3 DHCP REQUEST to obtain parameters

If the outbound DHCP server does not support DHCPINFORM the CNG may fall back on a DHCPREQUEST with the credentials of the CND. If this method is supported the CNG must send a DHCPREQUEST message with the IP address of the CNG in the "server identifier" field to decline the offered IP address but use the offered parameters for the inbound device. This is described in RFC 2131 [23], clauses 3.1.5 and 4.3.2, first list item (DHCPREQUEST generated during SELECTING state).

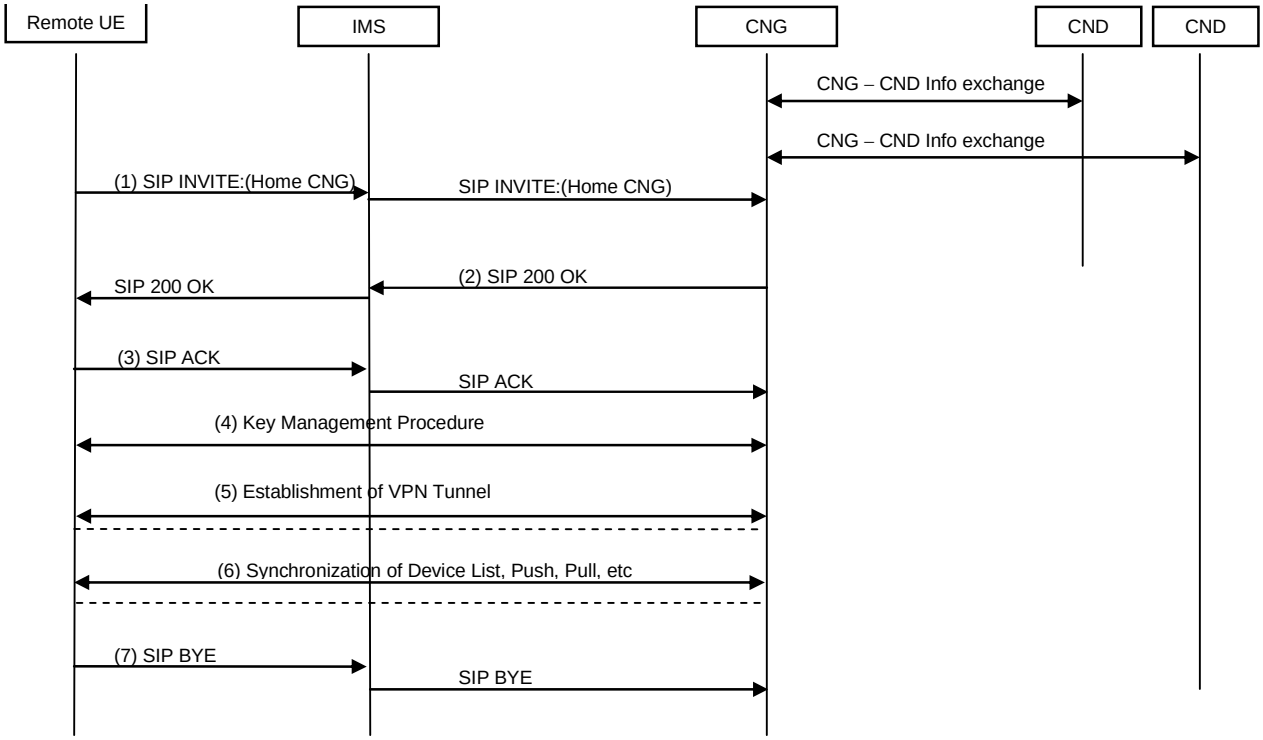
Annex A (normative): Remote Access Procedures

This clause is specifying procedures for Remote Access on the Gm reference point.

A.1 Remote Access Signalling

Based on IMS, using the Gm reference point conforming to ES 283 003 [5] for Remote Access, the Transport Agent, RATA is used for establishment of a communication channel enabling the Remote Access media flow between the remote UE and the CNG for extracting the home network to a remote location.

The remote access media flow can either be encrypted or unencrypted. As soon as it is established, normal UPnP™ procedures using the C reference point are used. Example of such operations is synchronization of device list, push and pull of content. An application in the UE supports the available RA services, including e.g. download and upload of content.



NOTE: Step (4) and (5) may not be used for unencrypted remote access media flow.

Figure A.1.: Remote Access establishment and actions

Prerequisite, in order to not have an empty device list, the CNDs in the CPN have to be registered (e.g. using UPnP™) to the CNG before the following take place:

1) The UE using the remote access menu initiates a SIP INVITE towards the Home CNG. The request is granted by the IMS core and sent to CNG.

   In order to inform the CNG that this INVITE is for a Remote Access (RA) session the SDP contains the following.

   The "c" connection, contains the IP address of the Remote Access Client (RAC).

   The "m" media, contains application defined as UDP, port number and the RA indication (vnd.etsi.ims.ra) proposed by the RAC within the UE.

   The "b" bandwidth, contains the requested bandwidth, e.g. 384 kbps.

NOTE 1: The actual requested bandwidth depends on the application.

   The "a" attribute, contains the RA Profiles, offering the supported IPsec profiles and the shared key. In case of profile 4, cert value, which specifies the use of a fingerprint attribute, is contained. Additionally, attributes used with a profile, such as a fingerprint attribute, as specified in RFC 4572 [14], an udp-setup attribute or a psk-fingerprint attribute, as defined in draft-saito-mmusic-sdp-ike-03 [3] in profile 4, should also be specified.

   Optionally, the "a=ra-client-private" attribute ip with values for IP and netmask. Since UEs might have other connections, this contains the client's network number and netmask for each LAN network interface connection the client is handling. In the example below the client has one LAN network interface, hence one entry pair.

NOTE 2: The value of the fingerprint attribute is a hash of the DER form of a certificate that is linked to the peer and will be used in the following key management procedure and VPN establishment. The fingerprint attribute is specified for the session or the media in RFC 4572 [14], depending on in which part of SDP it is specified, but is not linked to the specific ra-profile. The detail of the use of a fingerprint attribute and other associated attributes for IKE negotiation are described in draft-saito-mmusic-sdp-ike-03 [3].

NOTE 3: The absence of a cert or a key value in the SDP part indicates that the prior exchange of trusted certificates or shared secrets between connecting endpoints have been achieved in an out-of-band negotiation.

EXAMPLE 1: Example of an SDP that is compliant with the above specified text:

```
v  =  0
o  =  - 24351 621812 IN IP4 172.21.0.1

T  =  0 0
c  =  IN IP4 172.21.0.1
a  =  ra-client-private: ip=192.168.2.1 netmask=255.255.255.0
m  =  application 4500 udp vnd.etsi.ims.ra
b  =  AS:384
a  =  ra-profile: 1 key= LX1mY6iKA1n
a  =  ra-profile: 2 key= LX1mY6iKA1n
a  =  ra-profile: 3 key= LX1mY6iKA1n
a  =  ra-profile: 4 cert=fingerprint
a  =  fingerprint: SHA-1: 4A:AD:B9:B1:3F:82:18:3B:54:02:12:DF:3E:5D:49:6B:19:E5:7C:AB
```

2) CNG validates if the request for RA services shall be granted or rejected, using the P-asserted-Id added by the IMS core, asserting the remote UE's public ID (IMPU) and the Access Control List (ACL). The CNG-SIP Proxy B2BUA allocates IP-addresses and ports and prepares for the remote access procedures by returning SIP 200 OK.

   If the remote UE's public ID (IMPU) present in the INVITE request is not listed in the ACL the CNG shall respond with a SIP Response containing response code 403 (User Not Authorized). If the P-asserted-Id-header is missing the CNG shall respond with SIP Response containing response code 403 (User Not Authenticated).

   Regarding the offered setup profiles, if the CNG does not support any of the profiles in the client's SDP offer the CNG shall send a response with SIP Response containing response code 488 (Not Acceptable Here).

   If the maximum number of allowed connections has been reached the response given shall be SIP Response containing response code 486 (Busy Here).

   If the CNG detects that at least one network interface provided by the client is colliding with its own network address range it will dismiss the INVITE received. Two networks collide when minimum one IP-address belongs to both networks. The Response given shall be a SIP Response containing response code 488 (Not Acceptable Here) together with a Warning header field value explaining why the offer was rejected.

   In the response back the following is located in the SDP:

   - The "c" connection, contains the IP address of the CNG-SIP Proxy B2BUA NGN side.
   - The "m" media, contains application defined as UDP, port number and the RA indication (vnd.etsi.ims.ra).
   - The "a" attribute, contains:
     - the RA profile for the supported transport setup.
     - the LAN IP address for the remote client.

   Additionally, attributes used with the selected profile, such as a fingerprint attribute or a udp-setup attribute in profile 4, should also be specified in the response.

EXAMPLE 2: Example of an SDP when profile 1 is selected:

```
v = 0
o = - 34561 76531 IN IP4 172.23.0.1
t = 0 0
c = IN IP4 172.23.0.1
m = application 4500 udp vnd.etsi.ims.ra
b = AS:384
a = ra-profile: 1
a = ra-virtualip:IN IP4 192.168.1.49
```

EXAMPLE 3: Example of an SDP when profile 4 is selected:

```
v = 0
o = - 34561 76531 IN IP4 172.23.0.1
t = 0 0
c = IN IP4 172.23.0.1
m = application 4500 udp vnd.etsi.ims.ra
b = AS:384
a = ra-profile: 4 cert=fingerprint
a = fingerprint: SHA-1: D2:9F:6F:1E:CD:D3:09:E8:70:65:1A:51:7C:9D:30:4F:21:E4:4A:8E
```

3) SIP ACK is sent to acknowledge the Remote Access session setup. At this point a client may detect a possible address collision. An address collision occurs when the offered IP is already in use for other purposes on the client side, therefore making routing impossible to perform. If the client cannot handle this an error message should be sent to the user and the tunnel setup should not proceed. Immediately after the SIP ACK is sent, a SIP BYE message should be sent to terminate the session.

NOTE 4: By using IPv6 the address collisions would be eliminated.

4) If no keys for the tunnel where distributed in the SDP part the key management procedures commence agreeing on keys and tunnel type.

5) A secure tunnel is setup between the remote UE and the CNG enabling Remote Access services. The CNG-SIP Proxy B2BUA tells (internal implementation specific signalling) the CNG-PPF that the tunnel is available and where to find the remote client's RADA.

6) After tunnel establishment the discovery agent in the CNG, RAS, sends its IP address and port to the remote access client, RAC. Then any side may send synchronization messages.

NOTE 5: Upon availability of UPnP™ Remote Access architecture specifications they should be used for synchronization with the remote client.

The remote UE and different devices within the CPN are now in connection and various services can be handled. Examples are downloading and upload of content respectively. See clause 6.1.1.2 and onwards for information about e.g. push and pull services.

7) The Remote Access session is terminated, with SIP BYE.

A.2 VPN Tunnel Profiles

Four profiles are used for the setup of the VPN connection enabling the requested tunnel. The first two profiles are intentionally described and structured to be in alignment with the draft "RATAConfig: 1 Service" [i.1], which is accessible to UPnP members. The present document is however self-sufficient and the template format assumed in this document is based on certificate usage, using two options, both based on IP security (IPsec) The first profile provides authentication, integrity and encryption while the second profile is without support for encryption. Third option provides a Layer 2 Tunnel Protocol (L2TP) profile. First three profiles are using a shared key. Fourth profile uses fingerprint attribute and the corresponding IKE authentication method as described in draft-saito-mmusic-sdp-ike-03 [3].

A.2.1 Profile 1: Setup of tunnel using IPsec profile, using shared key

Table A.1

IPsec configuration profile	
Policy	
Perfect Forward Secrecy	True
Replay Window Length	10
Protocol	ESP
Key Length	128
Default Encryption Algorithm (see note 1)	AES-CTR
Default Authentication Algorithm (see note 1)	HMAC-SHA-256-128
Lifetime, seconds	28800
kBytes	5000
IKE	
IKE version	IKEv2
Send Notification	True
Id Type	ID-KEY-D
IPsec Expire	True
Replay Detection	True
Internal Address	True
DPD Heartbeat	600
Keep alive	100
Rekeying Threshold	90
Protocol	IKE
Key Length	128
Default Algorithm (see note 1)	AES-CTR
Default Integrity Algorithm (see note 1)	HMAC-SHA-256-128

IPsec configuration profile	
Default Pseudo Random Function (see note 1)	HMAC-SHA-256
Group Description	MODP 3072
GroupType lifetime, seconds	28800
GroupType lifetime, Kbytes	500
Authentication Method	Shared Secret
Credential ID (see note 2)	100
NOTE 1: The Default term used in the table is specifying the minimum level of support regarding algorithms and methods requested. E.g. other algorithms can be agreed upon during the performed negotiation by the two endpoints. NOTE 2: The parameter Credential ID is not used when using shared key.	

A.2.2 Profile 2: Setup of tunnel using IPsec, no_encryption profile, using shared key

Table A.2

IPsec, no encryption profile	
Policy	
Perfect Forward Secrecy	True
Replay Window Length	10
Protocol	ESP
Encryption Algorithm	NULL
Default Authentication Algorithm (see note 1)	HMAC-SHA1-96
Lifetime, seconds	28800
kBytes	5000000
IKE	
IKE version	IKEv2
Send Notification	True
Id Type	ID-KEY-ID
IPsec Expire	True
Replay Detection	True
Internal Address	True
DPD Heartbeat	600
Keep alive	100
Rekeying Threshold	90
Protocol	IKE
Key Length	128
Default Algorithm (see note 1)	AES-CBC
Default Integrity Algorithm (see note 1)	HMAC-SHA1 96
Default Pseudo Random Function (see note 1)	HMAC-SHA1
Group Description	MODP 768
GroupType lifetime, seconds	28800
GroupType lifetime, KBytes	50000
Authentication Method	Shared Secret
Credential ID (see note 2)	100
NOTE 1: The Default term used in the table is specifying the minimum level of support regarding algorithms and methods requested. E.g. other algorithms can be agreed upon during the performed negotiation by the two endpoints. NOTE 2: The parameter Credential ID is not used when using shared key.	

A.2.3 Profile 3: Setup of tunnel using L2TP/IPsec profile, using shared key

Table A.3

IPsec, configuration profile	
Policy	
Encapsulation Mode	Transport
Replay Window Length	10
Protocol	ESP
Key Length	128
Default Encryption Algorithm (see note 1)	3DES-CBC
Default Authentication Algorithm (see note 1)	HMAC-SHA1-96
Lifetime, seconds	28800
kBytes	5000
IKE	
IKE version (see note 2)	IKEv1
Send Notification	True
Id Type	ID-IPV4_ADDR
IPsec Expire	True
Replay Detection	True
Internal Address	True
DPD Heartbeat	600
Keep alive	100
Rekeying Threshold	90
Protocol	IKE
Key Length	128
Default Algorithm (see note 1)	3DES-CTR
Default Integrity Algorithm (see note 1)	HMAC-SHA1-96
Default Pseudo Random Function (see note 1)	HMAC-SHA1
Group Description	MODP 3072
GroupType lifetime, seconds	28800
GroupType lifetime, Kbytes	500
Authentication Method	Shared Secret
Credential ID (see note 4)	100
NAT-T	YES
Phase 1 Exchange	ID Protection Exchange(MainMode)
Port (in ID payload)	1702 (L2TP)
IKE SA situation	SIT_ID_ONLY
L2TP	
Version Revision Securing L2TP using IPsec (RFC 3193 [66]) Proxy Authentication	1 0 YES NO
PPP (see note 3)	
Default Username	"ra"
Default Password	"ra"
IPCP Server assigns IP to client PPP IPCP Extensions for name server addr Default Authentication Method (see note 1)	YES YES YES CHAP
NOTE 1: The Default term used in the table is specifying the minimum level of support regarding algorithms and methods requested. E.g. other algorithms can be agreed upon during the performed negotiation by the two endpoints. NOTE 2: IKEv2 is not available in all operating systems, even in the versions released in year 2009. NOTE 3: PPP is used as a part of the L2TP tunnel, a user name and password are required by the protocol but since they do not add to the security they are both set to default containing the string "RA". NOTE 4: The parameter Credential ID is not used when using shared key.	

A.2.4 Profile 4: Setup of tunnel using IPsec profile, using fingerprint attributes

Table A.4

IPsec RSA Digital Signature authentication profile	
Policy	
Perfect Forward Secrecy	True
Replay Window Length	10
Protocol	ESP
Default Encryption Algorithm (see note 1)	AES-CBC
Key Length	128
Default Integrity Algorithm (see note 1)	HMAC-SHA1-96
Lifetime, seconds	28800
Lifetime, kBytes	5000
IKE	
IKE version	IKEv2
Send Notification	True
Id Type	ID_KEY_ID
IPsec Expire	True
Replay Detection	True
Internal Address	True
NAT Probe	True
DPD Heartbeat	600
NAT Keep alive	120
Rekeying Threshold	90
Protocol	IKE
Default Encryption Algorithm (see note 1)	AES-CBC
Key Length	128
Default Integrity Algorithm (see note 1)	HMAC-SHA1-96
Default Pseudo Random Function (see note 1)	HMAC-SHA1
Group Description	MODP 2048
Lifetime, seconds	28800
Lifetime, Kbytes	5000
Default Authentication Method (see note 2)	RSA Digital Signature
NOTE 1: The Default term used in the table is specifying the minimum level of support regarding algorithms and methods requested. E.g. other algorithms can be agreed upon during the performed negotiation by the two endpoints. NOTE 2: The default authentication method is used if no fingerprint attribute or psk-fingerprint attribute was specified in SDP negotiation. Prior negotiation of a trusted CA certificate is assumed in the default authentication method.	

NOTE: SDP attributes that are described in draft-saito-mmusic-sdp-ike-03 [3] can be used if this profile is specified in SDP offer and answer.

A.3 ICSI for IMS RA Service

The IMS Communication Service Identifier (ICSI) uniquely identifies the IMS service and associated SIP procedures. The IMS communication service contains the service logic represented in the protocols used, see ES 283 003 [5] (TS 124.229 [20]).

URN used to define the ICSI for the "IMS Remote Access Service": urn:urn-7:3gpp-service.ims.icsi.ra.

The URN is registered at http://www.3gpp.org/Uniform-Resource-Name-URN-list.

Summary of the URN: This URN indicates that the device supports the IMS Remote Access Service.

A.3.1 Session Control Procedures

The ICSI may be supported to differentiate the procedures for RA service in relation to other IMS services.

If the ICSI is used the following applies:

a) "RA" is an IMS communication service and the P-Preferred-Service and P-Asserted-Service headers shall be treated as described in TS 124 229 [91], clause 8.4.1. The coding of the ICSI value in the P-Preferred-Service and P-Asserted-Service headers shall be as described in clause 7.2A8.2 of TS 124 229 [92].

b) The UE shall include the g.3gpp.icsi-ref feature tag equal to the ICSI value defined in clause 7.2A8.2 in the P-Preferred-Service header field in initial requests and responses as described in TS 124 229 [93], clause 8.4.1.

c) The UE shall include the g.3gpp.icsi-ref feature tag equal to the ICSI value defined in clause 7.2A8.2 in the Contact header field in initial requests and responses as described in TS 124 229 [94].

d) The UE shall include an Accept-Contact header field containing the g.3gpp.icsi-ref feature tag containing the ICSI value as defined in clause 7.2A8.2 of TS 124 229 [95] in initial requests. If the user requests capabilities other than RA, the Accept-Contact header field may contain other feature parameters and feature parameter values and other Accept-Contact header fields may be added to accurately express user preferences as per TS 124 229 [96].

Annex B (normative): Referenced Procedures on Gm

This clause is specifying procedures on Gm that are referenced from clause 7.

For each procedure, two columns are provided for the specification reference.

The first column is referencing the 3GPP specifications constituting TISPAN NGN Release 2 (based on TS 124 229 [20] Release 7).

The second column is referencing the 3GPP Release 8, which is defined after the TISPAN NGN Release 2.

Table B.1

Procedure Name	TISPAN NGN Release 2 specification	3GPP Release 8 specification
Basic Call	TS 124 503 [22], and TS 124 528	TS 124 229 [20], and TS 124 628 [74]
Communication Diversion	TS 124 504 [8]	TS 124 604 [75]
Communication Rejection	TS 124 411 [9]	TS 124 611 [76]
Explicit Communication Transfer	TS 124 529 [10]	TS 124 629 [77]
Communication Hold	TS 124 410 [11]	TS 124 610 [78]
Conference	TS 124 505 [67]	TS 124 605 [79]
Message Waiting Indication	TS 124 406 [13]	TS 124 606 [80]
Originating Identification	TS 124 407 [27]	TS 124 607 [81]
Terminating Identification	TS 124 508 [19]	TS 124 608 [82]
Malicious Communication Identification	TS 124 516 [68]	TS 124 616 [83]
Advice of Charge	TS 124 447 [69]	TS 124 647 [84]
Closed User Groups	TS 124 454 [70]	TS 124 654 [88]
DTMF	TS 124 503 [22]	TS 124 229 [20]
User Capabilities	TS 124 503 [22]	TS 124 229 [20]
Presence	TS 124 430 [71]	TS 124 141 [85]
Instant Messaging	TS 124 441 [72]	TS 124 247 [86]
SMS/MMS	TS 123 521 [73]	TS 124 341 [87]

History

Document history		
V2.1.1	July 2009	Publication