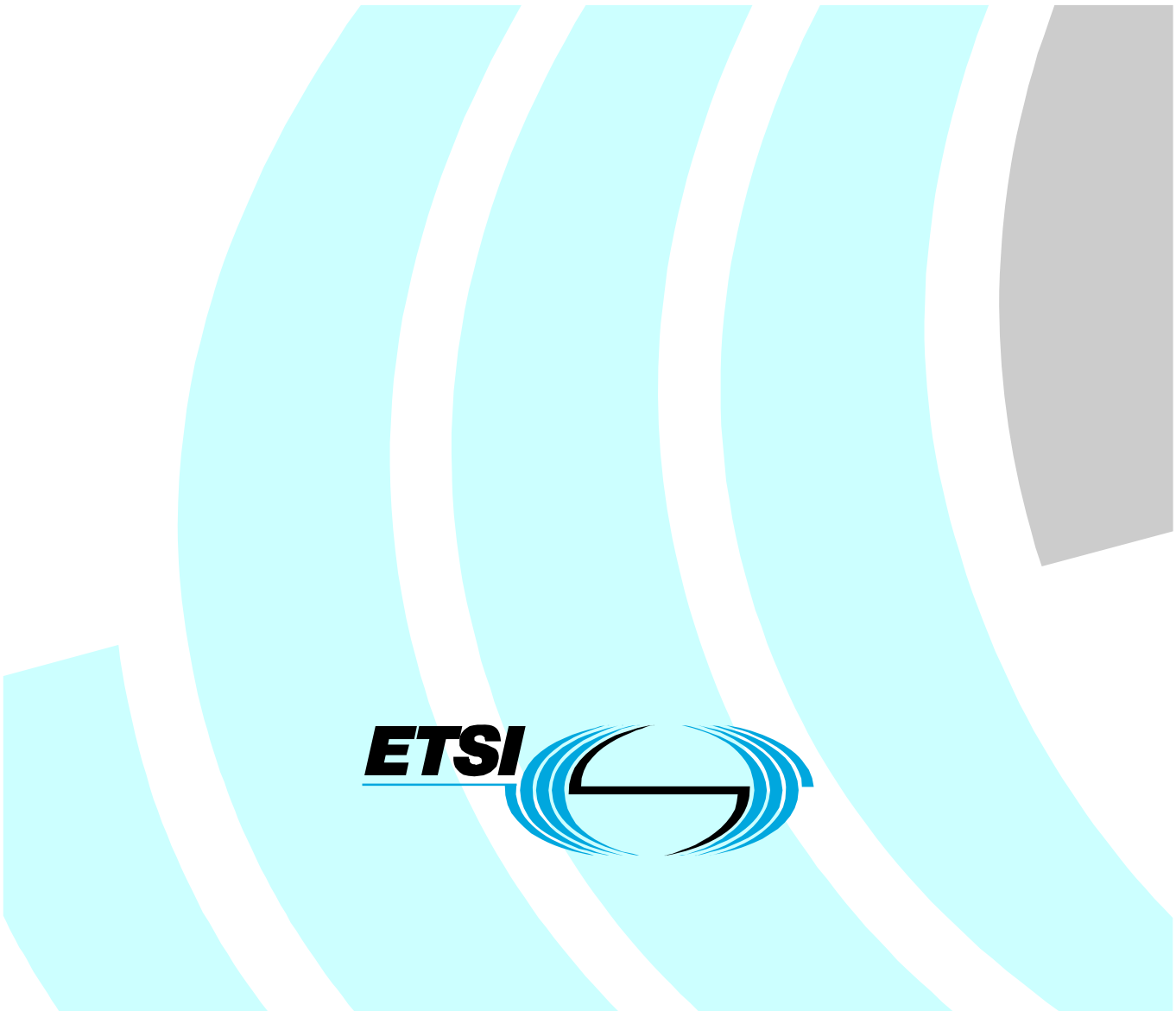
ETSI TS 185 003 V2.3.1 (2009-06)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Customer Network Gateway (CNG) Architecture and Reference Points



Reference
RTS/TISPAN-05023-NGN-R2

Keywords
architecture, gateway, IMS, interface, network

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 5
Foreword 5
Introduction 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 7
3 Definitions and abbreviations 8
3.1 Definitions 8
3.2 Abbreviations 8
4 The CNG Architecture 9
4.1 Introduction 9
4.2 CPN and NGN side requirements 10
4.2.1 Analogue phone connected to the NGN through a CNG 10
4.2.2 IMS Customer Network Device connected to the NGN through a CNG 11
4.2.3 SIP-non IMS Customer Network Device connected to the NGN through a CNG 12
4.3 CNG functions 13
4.3.1 The transfer level functions 13
4.3.1.1 CNG-NFF: CNG-NAPT and Firewall Function 13
4.3.2 The transport level functions 13
4.3.2.1 CNG-CSMF: CNG-Communication Services Media Function 13
4.3.2.2 CNG-IPTVF: CNG-IPTV Function 13
4.3.3 The CNG Network Attachment Subsystem entities (CNG-NASS) 13
4.3.3.1 CNG-CMF: CNG-Configuration and Management Function 13
4.3.3.2 CNG-AtF: CNG-Attachment Function 14
4.3.3.3 CNG-PCF: CNG-Policy Control Function 14
4.3.3.4 CNG-AuF: CNG-Authentification Function 14
4.3.3.5 CNG-LF: CNG-Location Function 14
4.3.4 The CNG-Resource and Admission Control Functional entities (C-RACF) 14
4.3.4.1 CNG-ACF: CNG-Admission Control Function 14
4.3.5 The CNG-Service-related Functional entities (CNG-SF) 15
4.3.5.1 VGCF: Voice Gateway Control Function 15
4.3.5.2 CNG-SIP Proxy B2BUA Function 15
4.3.5.3 CNG-PPF: CNG-Plug and Play Function 15
4.3.5.4 CNG-UIF: CNG-User Interface Function 16
4.3.5.5 ISIM module 16
5 The CNG Reference points 17
5.1 CND side Reference points 17
5.1.1 Network attachment reference points 17
5.1.1.1 e_1' reference point 17
5.1.1.2 e_3' reference point 17
5.1.1.3 a_u reference point 18
5.1.2 Transport level reference points 18
5.1.2.1 D_j reference point 18
5.1.2.2 Dj' reference point 18
5.1.3 Service-related reference points 18
5.1.3.1 G_m' reference point 18
5.1.3.2 u reference point 18
5.1.3.3 C reference point 19
5.2 NGN side Reference points 19
5.2.1 Network attachment reference points 19

5.2.1.1 e_1 reference point 19
5.2.1.2 e_3 reference point 19
5.2.2 Service-related reference points 19
5.2.2.1 G_m reference point 19
5.2.2.2 U_t reference point 20

6 The CNG Data Model 20

7 Information flows 20
7.1 Attachment flows 21
7.2 Configuration and management flows 21
7.3 Signalling flows 22
7.3.1 CND attachment and local/IMS registration 22
7.3.2 Outgoing call 24
7.3.2.1 SIP non-IMS CND 24
7.3.2.2 IMS CND 25
7.3.3 Internal call 25
7.3.4 Admission Control 26
7.4 Remote Access flows 28
7.4.1 Remote Access Connection Set-up 28
7.4.2 Download of content using HTTP 29
7.4.3 Upload of content using HTTP 30

Annex A (informative): Bibliography 32

Annex B (informative): Change History 33

History 34

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).

Introduction

The present document defines Release 2 of an anticipated series of releases of TISPAN NGN. Release 2 extends the capabilities of Release 1, enhances some Release 1 capabilities and provides some new services. The TISPAN NGN is described in terms of the content capabilities and this release (Release 2) is defined by the documentation set and the features that these support.

The general objective of Release 2 is to extend Release 1 through enhancements and new services. The present document focuses on additional capabilities and services and continues to enable an NGN to be a flexible platform allowing future enhancements and releases. The TISPAN NGN is specified using a release mechanism. The present document provides an overview of the capabilities in the second release. No assumptions should be made about future releases.

Throughout the present document, references to NGN are assumed to be references to TISPAN NGN unless otherwise indicated.

1 Scope

The present document provides an overview of Customer Network Gateway (CNG) functional architecture and reference points and the way it interacts with an NGN, as described in ETSI TISPAN Release 1 and Release 2 standards (see ES 282 001 [1]).

The present document describes architectural building blocks to be included in the CNG to support the interworking with an NGN, both at the transfer, transport and service layers. It also defines the reference points between the CNG internal architectural blocks involved and a CND.

The WG5 does not address the layer 1 issues, as such studies refer to the AT&TM Group.

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 ES 282 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture".

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

[3] ETSI ES 282 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Sub-System (NASS)".

[4] ETSI ES 282 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IP Multimedia Subsystem (IMS); Functional architecture".

[5] ETSI ES 283 003: "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]".

[6] ETSI TS 182 012: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); IMS-based PSTN/ISDN Emulation Sub-system (PES); Functional architecture".

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

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

[9] ETSI TS 131 103: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Characteristics of the IP Multimedia Services Identity Module (ISIM) application (3GPP TS 31.103)".

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

[11] ETSI TS 124 229: "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 8.2.0 Release 8)".

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

[13] ETSI TS 185 009: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Architecture and reference points of a customer network device for IMS based IPTV services".

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

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] ETSI TR 185 007: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Analysis of protocols for customer networks connected to TISPAN NGN".

[i.2] ETSI TR 185 004: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); High level customer network architectures".

[i.3] Broadband Forum TR-069: "CPE WAN Management Protocol".

[i.4] Broadband Forum TR-098: "Data Model for TR-069".

[i.5] Broadband Forum TR-104: "Provisioning Parameters for VoIP CPE".

[i.6] ETSI TS 185 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Services requirements and capabilities for customer networks connected to TISPAN NGN".

[i.7] ETSI TR 180 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Release 1; Release definition".

3 Definitions and abbreviations

3.1 Definitions

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

CPN Device: device that is physically installed in the CPN allowing user access to network services; this can be a Customer Network Gateway with gateway functionalities towards the NGN, or a Customer Network Device being the end user terminal

Customer Network Device (CND): CPN device enabling the final user to have direct access to services through a specific user interface

NOTE: CNDs can be dedicated to the internet, conversational and audio-video services. But they could be also Consumer Electronics equipment and other devices which may have nothing to do with these premium services (e.g. services performing a content sharing within a CPN, typically between a PC and a music system).

Customer Network Gateway (CNG): CPN device acting as a gateway between the CPN and the NGN

NOTE: CNG is able to perform networking functions from physical connection to bridging and routing capabilities (L1 to L3), but also possibly implementing functions related to the service support (up to L7).

Customer Premises Network (CPN): in-house network composed by customer network gateway, customer network devices, network segments, network adapters and nodes

NOTE: Network segments are physical wired or wireless connections between customer premises network elements); network adapters are elements performing a L1/L2 conversion between different network segments; nodes are network adapters with L3 routing capabilities.

IMS CND: CND whose external behaviour complies with the IMS specifications

NOTE: See [1], [2], [3], [4] and [5].

"Multiple" Play Services (can be: double, triple, quadruple etc.): delivery by a single service provider of different types of concurrent services to one or multiple users within the same CPN

NOTE: Services can be categorized in the following way: data (e.g. Web browsing, best effort traffic etc.), person(s) to person(s) communication, entertainment.

Non-IMS SIP IETF CND: SIP-based CND whose external behaviour conforms to RFC 3261 [8] but do not fully conform to the IMS specifications

Many scenarios are expected to provide one service from a service provider to a customer device (case of multiple service providers, one or several CNG, etc.). They are presented within the TR 185 004 [i.2] and TS 185 005 [i.6].

3.2 Abbreviations

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

ACS	Auto-Configuration Server
AKA	Authentication and Key Agreement
ALG	Application Layer Gateway
A-MGF	Access-Media Gateway Function
ARF	Access Relay Function
B2BUA	Back-to-Back User Agent
BC	Broadcast Content
CLF	Connectivity session Location and repository Function
CND	Customer Network Device
CNG	Customer Network Gateway
CNG-ACF	CNG-Admission Control Function
CNG-AtF	CNG-Attachment Function

CNG-AuF	CNG-Authentication Function
CNGCF	CNG Configuration Function
CNG-CMF	CNG-Configuration and Maintenance Function
CNG-CSMF	CNG- Communication Services Media Function
CNG-LF	CNG-Location Function
CNG-NFF	CNG-NAPT and Firewall Function
CNG-PCF	CNG-Policy Control Function
CNG-PPF	CNG-Plug and Play Function
CNG-UIF	CNG-User Reference point Function
CoD	Content on Demand
CPN	Customer Premises Network
DHCP	Dynamic Host Configuration Protocol

NOTE: http://www.ietf.org/rfc/rfc3235.txt?number=2131

DLNA	Digital Living Network Alliance
EF	Elementary Files
ETH	ETHernet
IGMP	Internet Group Multicast Protocol
IMPU	IMS PUblic identity
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPTV	IP TeleVision
ISIM	IMS Subscriber Identity Module
MGC	Media Gateway Controller
NACF	Network Access Configuration Function
NAPT	Network Address and Port Translation

NOTE: http://www.ietf.org/rfc/rfc3235.txt?number=3235

NASS	Network Attachment Subsystem
NAT	Network Address Translation
NDN	Next Generation Network
P-CSCF	Proxy Call Session Control Function
PLT	Power-Line Telecommunication
RADA	Remote Access Discovery Agent
RATA	Remote Access Transport Agent
RTSP	Real Time Streaming Protocol
SDP	Session Data Protocol
SIP	Session Initiation Protocol
SSID	Service Set IDentifier
UE	User Equipment
UICC	Universal Integrated Circuit Card
VGCF	Voice Gateway Control Function
VoIP	Voice over IP

4 The CNG Architecture

4.1 Introduction

The following clauses present the functional entities for the CNG. Examples of Customer Network Devices may be connected to the CNG:

a) Analogue phones connected through the CNG to the NGN network.

b) IMS Customer Network Devices connected through a CNG to the NGN network [5].

c) Non IMS SIP IETF Customer Network Devices [7].

d) ISDN Customer Network Devices through the CNG to the NGN network.

Different types of Customer Network Devices may be involved in Intra CPN communication through a CNG.

The list of Customer Network Devices which are likely to be connected to the CNG is provided by the TS 185 006 [12].

The general overview of the CPN Architecture is provided by the TR 185 004 [i.2]. The CNG functional entities are described in the following parts of the document, as well as the reference points between each function.

4.2 CPN and NGN side requirements

The list of the CNG requirements is provided by the TS 185 005 [i.6]. specification for Service requirements and capabilities for customer networks connected to TISPAN NGN.

4.2.1 Analogue phone connected to the NGN through a CNG

In this case, the CNG includes all the CPN functionalities necessary to fulfill a service between the analogue phone and the NGN, as shown in figure 1.

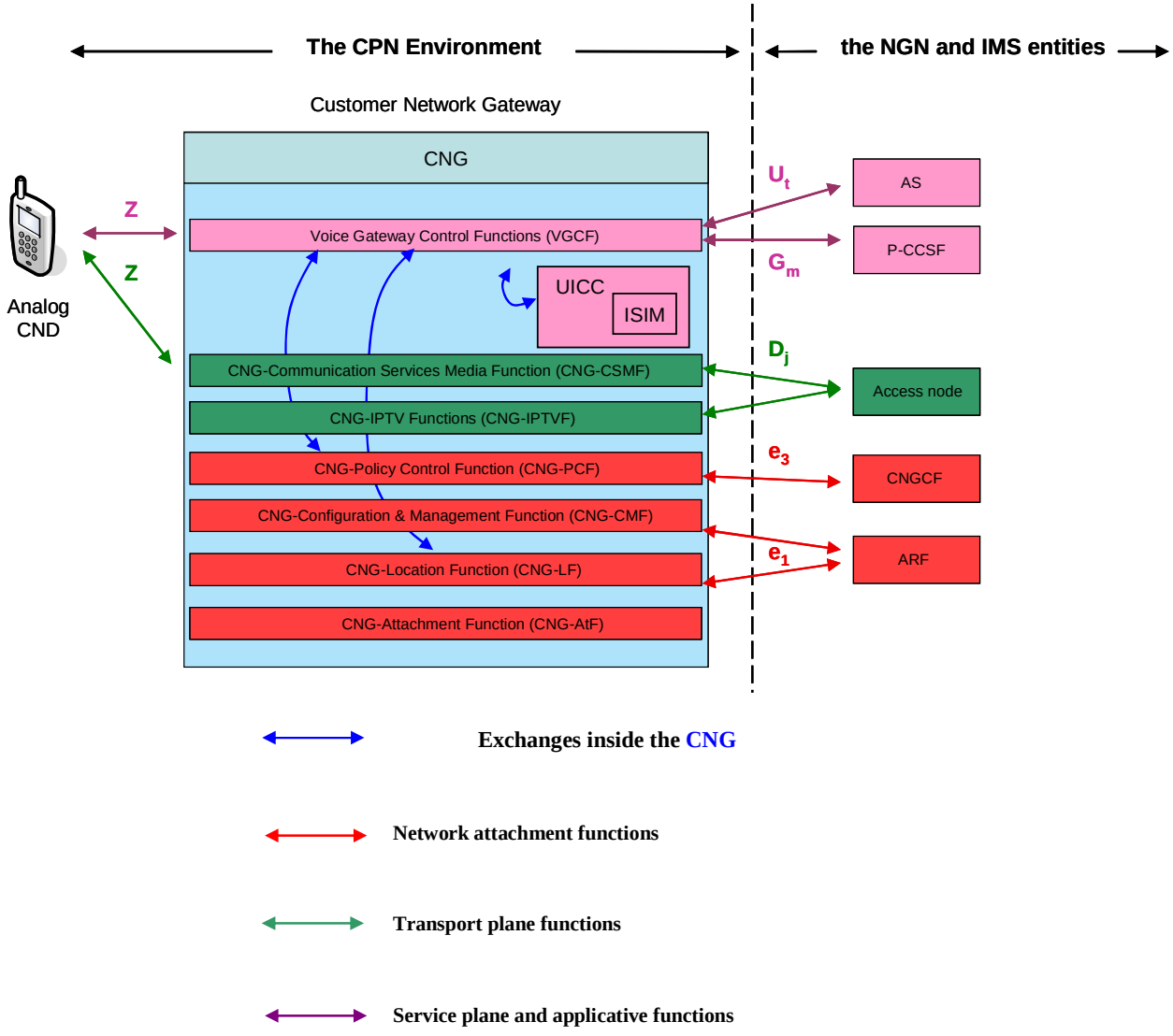
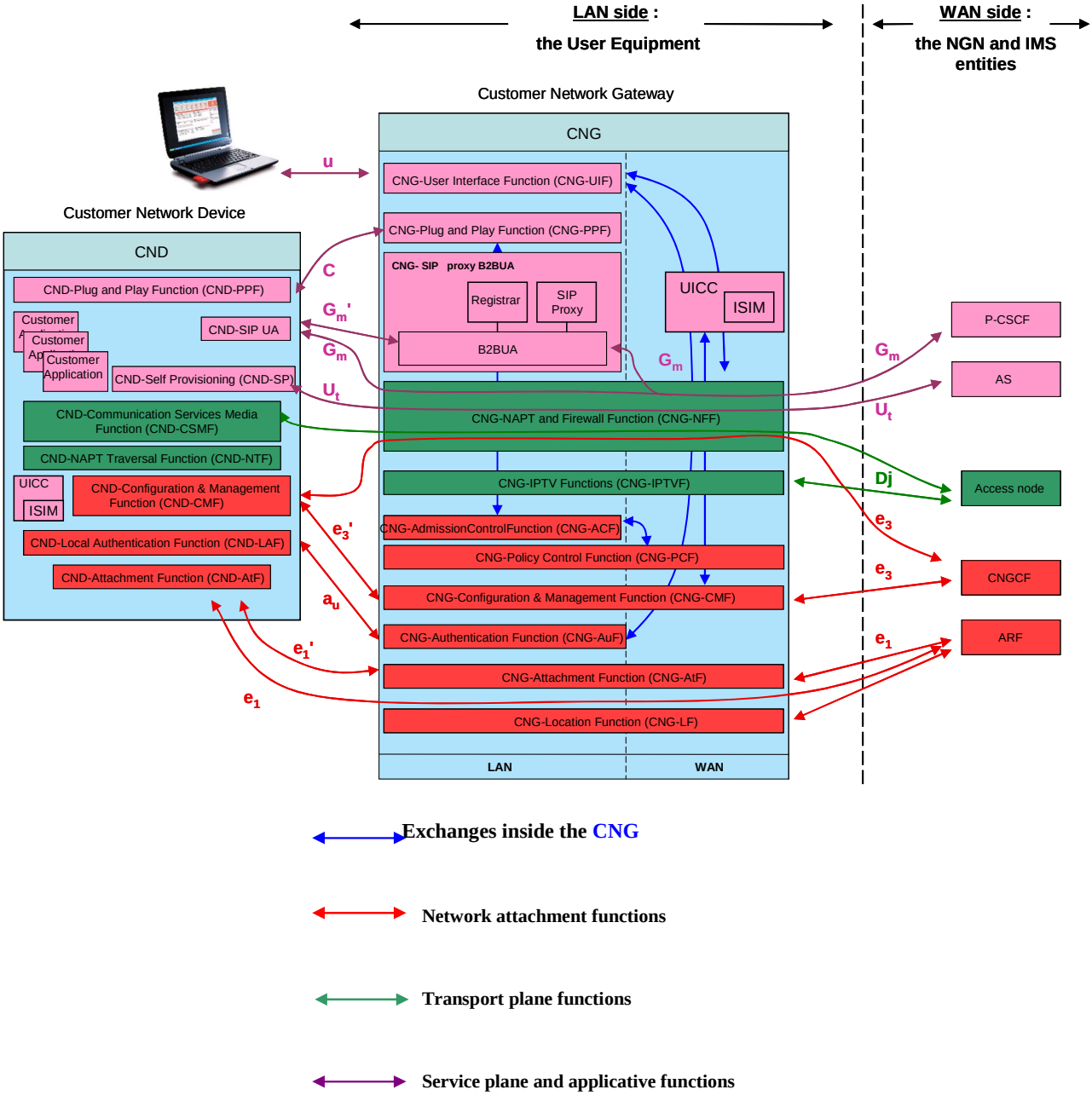


Figure 1: Analogue phone connected to the NGN-IMS network through a CNG

4.2.2 IMS Customer Network Device connected to the NGN through a CNG

In this case, the Customer Network Device includes all the CPN functionalities necessary to fulfilll a service between itself and the NGN-IMS network, as shown in figure 2:



NOTE: The IMS CND functions are described within TS 185 006 [12] dedicated to Customer Network Devices.

Figure 2: IMS Customer Network Device connected to the NGN-IMS network through a CNG

4.2.3 SIP-non IMS Customer Network Device connected to the NGN through a CNG

In this case, the Customer Network Gateway includes all the CPN functionalities necessary to fulfilll a service between itself and the NGN-IMS network, as shown in figure 3.

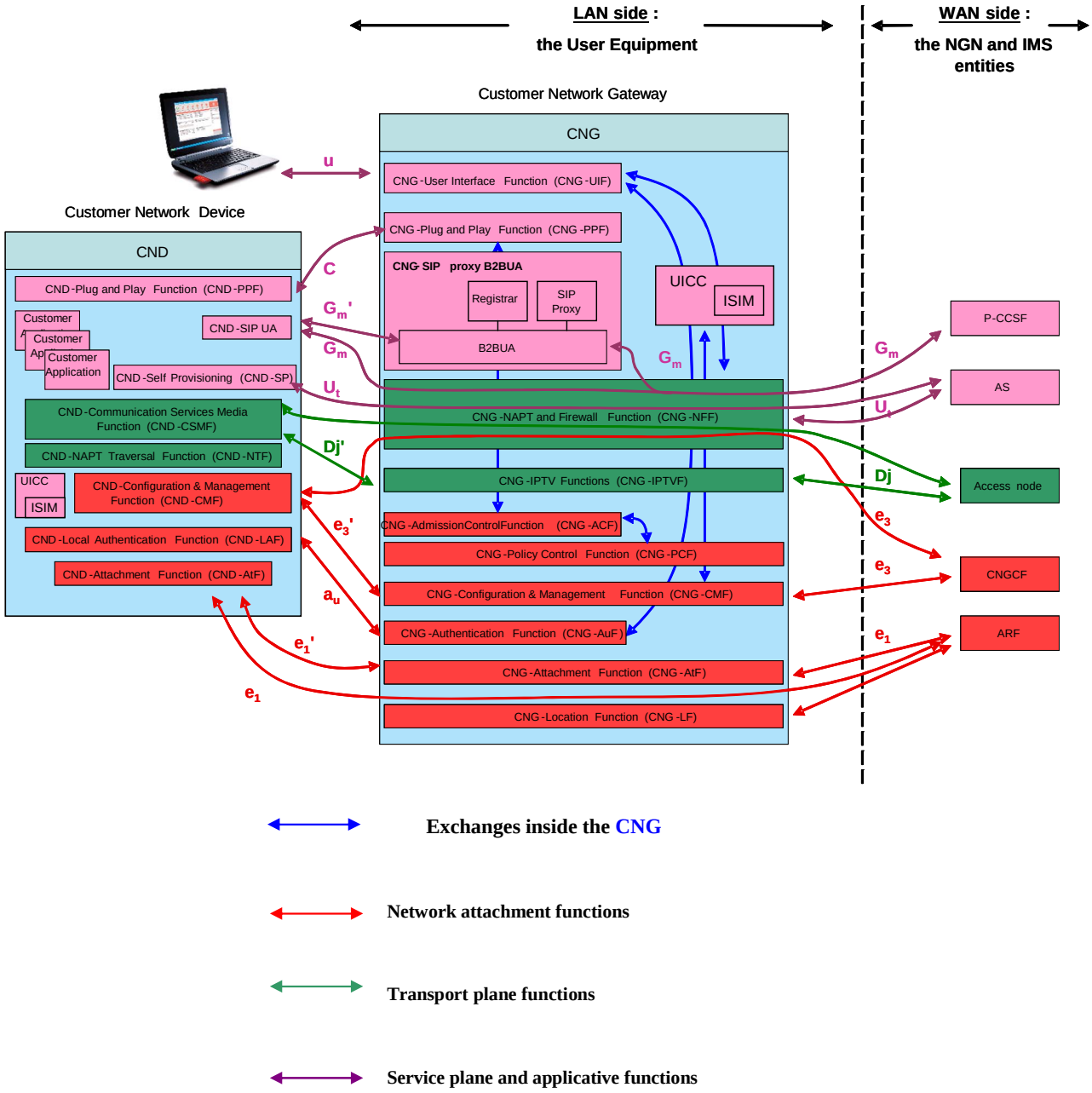


Figure 3: Non IMS SIP Customer Network Device connected to the NGN-IMS network through a CNG

In this case G_m' is used, the SIP proxy B2BUA shall perform an adaptation of the non-IMS SIP profile from a CND which requests for an IMS session.

4.3 CNG functions

4.3.1 The transfer level functions

4.3.1.1 CNG-NFF: CNG-NAPT and Firewall Function

The CNG-NFF entity shall provide gate control functionality i.e. dynamic NAPT and firewall functions at the boundary between the CPN and the NGN.

4.3.2 The transport level functions

4.3.2.1 CNG-CSMF: CNG-Communication Services Media Function

The CNG-CSMF is the termination point for the access node, it shall perform an adaptation so as to deliver media flows from the NGN network to an analogue or IP Customer Network Device.

The CNG-CSMF is used for analogue (or digital in the case of ISDN CNDs) to IP media conversion - in which case it corresponds to the R-MGF identified in ES 282 001 [1] or it is used for IP-IP media traffic.

In case the CPN is provided with analogue or ISDN CNDs and the media gateway function is not implemented in the NGN (as an A-MGF, c.f. ES 282 001 [1]), the CNG-CSMF shall be used.

As a result, this functionality is recommended.

4.3.2.2 CNG-IPTVF: CNG-IPTV Function

When supporting IPTV services, the CNG shall be able to forward inbound multicast packets only to the physical interfaces connected to devices that have joined the specific multicast group. This mechanism should be implemented acting on layer 2 and layer 3 multicast signalling flows (e.g. IGMP based).

The CNG shall be able to perform a link layer multicast to unicast translation, if the CPN segment, which the IPTV CND is connected to, is not able to support multicast; specifically, when sending an IP multicast packet to a host received on an NGN reference point, the CNG can send the packet to the unicast MAC address of the host (contained in the multicast signalling message without any change in the IP destination address). This mechanism is also of interest for example when the IPTV CND is connected to the CNG through Powerlines technology (directly or using ETH-to-PLT bridges).

4.3.3 The CNG Network Attachment Subsystem entities (CNG-NASS)

4.3.3.1 CNG-CMF: CNG-Configuration and Management Function

The CNG-CMF shall manage a mutual authentication between the CNGCF and the CNG.

The CNG-CMF shall enable the CNG configuration and firmware upgrade.

The CNG-CMF entity should enable transmission of configuration information to CNDs, obtained from the CNGCF. As a result the CNG-CMF should be able particularly to store configuration information dedicated to several CND, after sending only one request to the CNGCF. As soon as a CND is connected, the CNG-CMF should be able to deliver configuration parameters to it.

Furthermore, the CNG-CMF should allow maintenance of any CPN device (CNG/CND) from the NGN network, through the CND-CMF, that is to say the opportunity to do diagnostic and performance tests too. Functionalities should be added to the CNGCF, whether this latter entity could perform the CPN maintenance.

For instance, the CNG-CMF could provide the functionality and reference points of a Broadband Forum Auto Configuration Client (see TR-069 [i.3]).

Moreover, the CNG-CMF may be able to perform management activities related to remote access. The remote access allows the user to access a CND from another device via the Internet through the G_m reference point, and work on it remotely.

Some authentication parameters may be stored in a UICC (containing the ISIM).

4.3.3.2 CNG-AtF: CNG-Attachment Function

The CNG-AtF entity shall be responsible for allocation of IP addresses to user premises equipment (CND), and to the CNG from the NACF via the ARF.

4.3.3.3 CNG-PCF: CNG-Policy Control Function

The CNG-PCF may integrate a database containing the access profile.

This includes bandwidth and QoS parameters for the CNG Customer Network Device side applications and terminals, which could be configured by a user. For instance, congestion issues within the CPN may be solved defining resources for several SSID.

4.3.3.4 CNG-AuF: CNG-Authentification Function

The CNG-AuF shall manage the authentication of CNDs to be connected to the CPN. A CND requesting for a CPN Wireless attachment should be authorized by the access point embedded in the CNG.

The CNG-AuF may thus be configured by the user for such a case, using the CNG-User Interface Function (CNG-UIF).

4.3.3.5 CNG-LF: CNG-Location Function

The CNG-LF functional entity may allow an internal application providing location information, to perform for instance emergency calls or deliver some local video content.

This information may be configured by the owner of the CNG, received from the CLF or obtained from the network, via the CNG-AtF (typically through DHCP option 82).

The information should also come from the CLF. In this case the CNG-LF may not be used.

4.3.4 The CNG-Resource and Admission Control Functional entities (C-RACF)

4.3.4.1 CNG-ACF: CNG-Admission Control Function

The CNG-ACF should receive and send QoS messages from/to the CNG-SIP proxy B2BUA Function. In particular it should:

a) check resources availability on each link/device involved in the communication requesting a QoS reservation/allocation, through an internal database;

b) perform the appropriate resources reservation, through the CNG-PCF.

Thus, the CNG-ACF should manage session limitations for instance or the priority of media streams. This applies to upstream flows but there may also be an opportunity to do so for downstream flows.

The CNG-ACF is only able to take into account sessions that pass through the SIP B2BUA. Sessions using encrypted signalling or different signalling protocols will not be included. In the latter case the CNG-ACF might allow more sessions through the access line that it should have. As RACS has a full view on all sessions over the access line, it will deny the session setup thus preventing an overload situation [i.7].

4.3.5 The CNG-Service-related Functional entities (CNG-SF)

Depending on the services supported, a CNG may include one or more Service-related Functions. The present version of the present document identifies four types of SCFs intended to support SIP-based applications. It should be noted that not all applications require a Service-related Function to be involved (e.g. P2P applications usually do not require such functions).

4.3.5.1 VGCF: Voice Gateway Control Function

The VGCF within the CNG is the equivalent of an MGC embedding a SIP User Agent. A CNG should include several UAs in case of multi analogue and/or ISDN Customer Network Device within the CPN. The VGCF should control the CNG-CSMF (i.e. the R-MGF as defined in ES 282 001 [1]).

The VGCF should perform the service authentication and manage signalling flows securely.

NOTE: The VGCF together with the CNG-CSMF provides the function of a R-VGW as defined in TS 182 012 [6].

In case of AKA authentication, the VGCF shall have access to the authentication parameters through an ISIM/UICC functionality. To be noticed that HTTP Digest is for an early deployment whereas IMS AKA is the target solution.

4.3.5.2 CNG-SIP Proxy B2BUA Function

The CNG-SIP Proxy B2BUA should implement:

a) a Local SIP Registrar without any authentication needed;

b) an outbound SIP Proxy, a SIP access point for the P-CSCF, forwarding the register messages to the P-CSCF if necessary.

Moreover, it may be:

c) a protocol adaptation module performing an adaptation of non-IMS compliant IETF SIP protocols towards one IMS compliant SIP protocol. This functionality could also be performed by the NGN.

NOTE: Some adaptation may be performed by the CNG so as to support non-IETF SIP CNDs in the CPN (proprietary SIP) but this case is out of the scope of the present document.

d) a protocol adaptation module performing remote access communication establishment. This functionality is called Remote Access Transport Agent (RATA).

The CNG-SIP Proxy B2BUA Function should be aware of each SIP CND (could be an IMS CND) capability within the CPN environment.

The CNG-SIP Proxy B2BUA Function shall at last be able to manage two SIP dialogues and the associated identities (possibly through an ISIM module), from both the NGN and the CND sides. This gives the opportunity to transfer an IMS session from a device to another or to forward an incoming call to the appropriate CNDs (forking).

The responsibility of the RATA is to provide a communication channel enabling interaction between remote and in the home network located UPnP capable CND's.

In case of AKA authentication, the SIP Proxy B2BUA shall have access to the authentication parameters through an ISIM/UICC functionality. To be noticed that HTTP Digest is for an early deployment whereas IMS AKA is the target solution.

4.3.5.3 CNG-PPF: CNG-Plug and Play Function

The CNG-PPF may obtain some CND information (service discovery, description) and allow their control.

Also, the CNG-PPF should allow a communication between many types of Customer Network Device within the CPN, not only conversational (based on UPnP for instance).

The CNG-PPF may also support this kind of communication through the CNG between NGN devices and CND devices.

While facilitating such communication, ALG functionality may be needed by the CNG-PPF, interfacing the CNG-NFF.

Since some of the communication sessions supported by the CNG-PPF result in media sessions, the CNG-PPF may need to interface the CNG-ACF in order to support QoS provisioning for these types of services.

The Remote Access Discovery Agent (RADA) discovers and maintains a device-list for the services provided. The list is continuously updated, kept and provided for facilitating communication between devices.

When sessions (for example UPnP based) are initiated between a CND and a remote NGN device, they may be established by IMS SIP session establishment and then described in the SDP parts of the IMS SIP signalling. When establishing the UPnP session between the NGN and CPN endpoints the CNG-PPF needs to perform ALG functionality, by re-writing any CPN references within the UPnP messages and also control port forwarding through the CNG-NFF. Informative flows for the Remote Access feature are detailed in clause 7.4.

4.3.5.4 CNG-UIF: CNG-User Interface Function

The CNG-UIF entity should allow the user to configure many CNG parameters for the transport layer:

a) firewall rules, possibly defined for each user (e.g. parental control);

b) CNDs authorized within the CPN, with possible bandwidth restrictions.

The operator shall be able to prevent a user from modifying a specific subset of CPN parameters.

Thus this entity may have reference points with the CNG-AuF and the CNG-NFF of the CNG.

4.3.5.5 ISIM module

The ISIM (see figure 4) is a network access application dedicated to IMS access contained in a UICC. It may be implemented in a CNG.

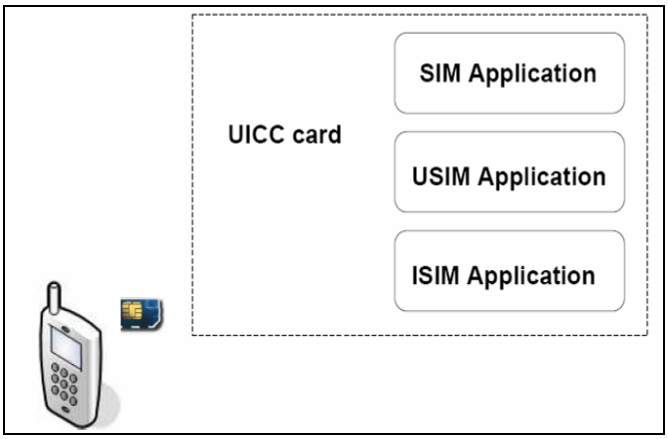


Figure 4: Example of "UICC Card composition"

The ISIM includes:

a) The IMPI (IMS private identity).

b) At least one IMPU (IMS public Identity).

c) The operator's NGN Domain Name.

d) Support for sequence number checking in the context of the IMS Domain.

e) The same framework for algorithms as specified for the USIM applies for the ISIM.

f) An authentication element so as to support the AKA authentication.

The ISIM is located in the ISIM Application Dedicated File (ADFISIM) and contains service and network related information. The ADFISIM provides various data contained in Elementary Files (EF), for instance the EFIMPI containing the private user identity. Details about this file structure can be found in TS 131 103 [9].

5 The CNG Reference points

5.1 CND side Reference points

5.1.1 Network attachment reference points

5.1.1.1 e_1' reference point

The e_1' reference point is defined between the CND and the CNG-AtF. The CNG-AtF provides IP addresses (IPv4 or IPv6 format) to the CND through the CND-AtF, it may also send some configuration information for the CND (typically through DHCP).

The CND and CNG shall mutually exchange their identities (e.g. MAC address, DeviceID, etc.) on e_1' reference point. The CNG has to know which CNDs are behind itself within the CPN and each CND has to know its CNG.

This reference point is mandatory if the CNG runs in a routed mode

5.1.1.2 e_3' reference point

The e_3' reference point is defined between the CND and the CNG-CMF. The CNG-CMF may provide the CND with parameters that are pre-configured in the CNGCF and sent to the CNG through the e_3 reference point or, as an alternative, directly defined by the user. The CNG-CMF also configures the CNG, using information received from the CNGCF or supplied by the user himself.

The CND should provide information on CND status to allow the CNGCF to make some diagnostic and performance tests through the CNG-CMF.

To sum up, the e_3' reference point supports a variety of functionality to manage a collection of user equipment (CNG/Customer Network Devices), including the following capabilities:

a) auto-configuration and service provisioning;

b) software/firmware management;

c) status and performance monitoring;

d) diagnostics.

This reference point is recommended as the e_3 reference point could also be used.

The above mention functionalities can be also implemented directly using a direct e_3 reference point between CND and CNGCF as an e_3 reference point defined in ES 282 004 [3].

The direct reference point between CND and CNG, e_3', could be limited to service provisioning functions; this may be used as an alternative to the corresponding functionalities on the e_3 reference point between CND and CNGCF.

5.1.1.3 a_u reference point

The a_u reference point is defined between the Customer Network Device and the CNG-AuF. There may be two types of authentication/authorization, according to:

a) CPN pairing (attachment, encryption and security processes (WEP, WPA2, etc.)) based on specific CPN technologies (e.g. Wifi SSID, PLC technology).

b) Access rights for some LAN services like the CNG Configuration (through the CNG-UIF).

This reference point is recommended, except if a wireless access point is embedded in the CNG in which case it is mandatory.

5.1.2 Transport level reference points

5.1.2.1 D_j reference point

The D_j reference point is responsible for the exchange of media flows between the User Equipment (CNG or CND) and the access node.

This reference point is mandatory. It is based on the ES 282 001 [1] specification.

5.1.2.2 Dj' reference point

The Dj' reference point is responsible for the exchange of media flows between the IPTV CND and the CNG. It is applicable only in case the CNG is supporting IPTV in routed mode, as specified in TS 185 009 [13].

Through Dj', the IPTV CND communicates with the CNG-IPTVF and its related functionalities (IGMP proxy and snooping).

This reference point is mandatory for IPTV CNDs performing CoD service (using RTSP) and BC service (using IGMP).

5.1.3 Service-related reference points

5.1.3.1 G_m' reference point

The G_m' reference point supports the communication between a CND and the CNG, e.g. related to registration and session control.

The difference between G_m and G_m' is related to the conformance to the IMS and to the need to go through the B2BUA to support local services. Further details about Gm' possible implementations can be found in the TR 185 007 [i.1].

This reference point is recommended.

5.1.3.2 u reference point

The u reference point gives the possibility to one or several users authorized (via the CNG-AuF) to have access to the CNG Configuration, through the CNG-UIF. The liaison should be as secure as possible (using HTTPs for instance).

This reference point is recommended.

5.1.3.3 C reference point

The C reference point is defined between the CNG-PPF and the CND-PPF.

It provides some CND information (service discovery, description) to the CNG and allow its control.

Also, a communication between many types of Customer Network Device within the CPN may be established through the C reference point, using UPnP for instance.

This reference point is optional.

5.2 NGN side Reference points

5.2.1 Network attachment reference points

5.2.1.1 e_1 reference point

This reference point is based on the TS 183 019 [7] specification.

The e_1 reference point is dedicated to the network attachment of the User Equipment.

The e_1 reference point is mandatory (in coherence with WG2 specifications).

5.2.1.2 e_3 reference point

This reference point is based on the ES 282 004 [3].

The e_3 reference point is defined between the CNG-CMF and the CNGCF and should be extended also between the CNG-CMF and the CND for configuration purposes.

Through a remote management protocol it is possible to support a variety of functionalities to manage a collection of user equipment (CNG/Customer Network Devices), including the following capabilities:

a) auto-configuration and service provisioning;

b) software/firmware management;

c) status and performance monitoring;

d) diagnostics.

The e_3 implementation between the CNG-CMF and the CNGCF is mandatory (in coherence with WG2 specifications), whereas the e_3 implementation between the CNG-CMF and the CND-CMF is recommended, as e_3' should be an alternative.

5.2.2 Service-related reference points

5.2.2.1 G_m reference point

The G_m reference point supports the communication between UE and the IMS, e.g. related to registration and session control.

G_m between the P-CSCF and the SIP proxy B2BUA is used to support several actions:

a) send SIP messages to/from the NGN;

b) call forking at the CNG level.

The protocol used for the G_m reference point is SIP.

To be noticed that the definition is extracted from the ES 282 007 [4].

This reference point is in line with the following specifications:

a) ES 283 003 [5].

b) TS 182 012 [6].

c) TS 131 103 [9].

This reference point is mandatory (in coherence with WG2 specifications).

5.2.2.2 U_t reference point

The U_t reference point enables the user to manage information related to his services, such as creation and assignment of Public Service Identities, management of authorization policies that are used e.g. by Presence service, conference policy management, etc.

This reference point is in line with the ES 282 007 [4].

This reference point is optional (in coherence with WG2 specifications).

6 The CNG Data Model

In case of an xDSL access network, the CNG shall support the gateway data model proposed by Broadband Forum in TR-098 [i.4] (data model for an internet gateway device).

In order to support IPTV CNDs, the CNG shall be compliant with Broadband Forum TR-069 [i.3] amendment 1 annex F
(device - gateway association) and in order to solve the NAT traversal problem for ACS initiated session setup the CNG shall support the dynamic port mapping creation function as specified in TR-098 [i.4].

In order to support non IMS CND, the CNG shall support the set of parameters defined by Broadband Forum in TR-104 [i.5] (data model for VoIP functionalities).

The data model for cable-based CNG is for further studies.

7 Information flows

NOTE: This clause is informative text reported in the form of examples, to give a better understanding of the relationships between the CPN entities and functionalities. Exhaustive information flows will be given in a stage 3 document.

7.1 Attachment flows

The candidate protocol on e_1' is DHCP specified in RFC 2131 [10]. In figure 5 the basic information flow is given.

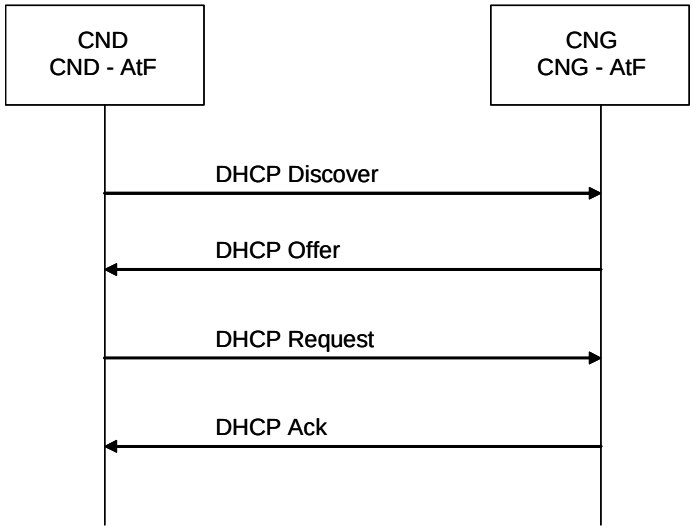


Figure 5: CND Attachment on e_1'

In order to mutually exchange the hardware identities between the CND and the CNG, the hardware identity can be defined for example as in TR-069 [i.3] (DeviceId) and the DHCP Option 125 can be used for the CND-CNG association as specified in TR-069, annex F [i.3].

7.2 Configuration and management flows

The following information flow is an example of service provisioning functions supported by CNG (see figure 6).

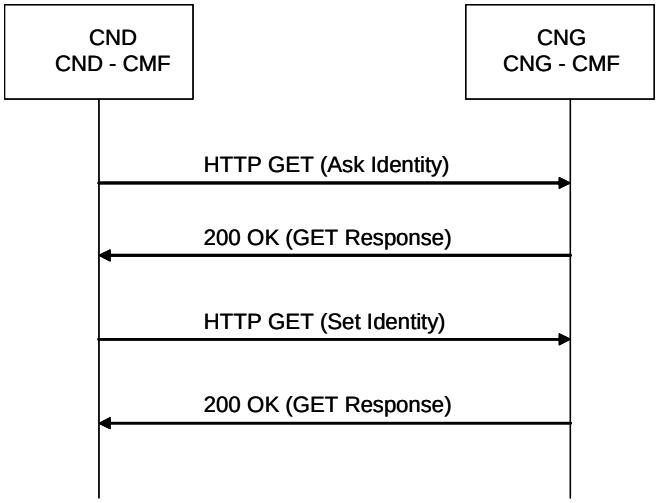


Figure 6: Provisioning on e3'

With the first HTTP GET (Ask Identity), the CND asks the CNG for the list of available identities (IMPI, IMPU, etc.), and the CNG answers with the identities list in the HTTP GET Response. Then the CND chooses one identity and, in the second HTTP GET (Set Identity), provides the choice to the CNG, which then answers with confirmation in the HTTP Get Response.

7.3 Signalling flows

The candidate protocol on G_m' is SIP specified in RFC 3261 [8], and optionally HTTP Digest as an authentication method as specified in RFC 2617 [14].

The candidate protocol on G_m is SIP specified in TS 124 229 [11] and ES 283 003 [5].

7.3.1 CND attachment and local/IMS registration

The non-IMS devices considered in this case are devices associated to the VoIP phone number of the CNG.

Different kinds of devices are foreseen (see also TS 185 006 [12]), some examples are:

a) Fixed or Wireless SIP phone.

b) SIP Multi-mode (e.g. dual WI-Fi/3G phone).

c) SIP softphone on PC.

d) Other: playstation, STB, etc.

These SIP non-IMS devices have a local SIP identity, as defined as local SIP URI (e.g. device_kitchen) or public SIP URI (e.g. John123):

a) Vendor provides a local SIP identity for all SIP devices. This enables "Plug and play" functionality. User does not need to configure the SIP device. By default, this local identity can be the MAC address.

b) User can change the local identity provided by the vendor to another local identity or public SIP URI. The customer can change this parameterization, and select a specific name.

Or a local phone number for each device.

The attachment phase is:

1) For non IMS CND's the G_m' reference point is used (for local services), the DHCP server of the CNG will return the DHCP option 120 to the CND, standardized to provision CNG SIP proxy IP address or domain-name. This option will contain the IP address of the CNG on the CPN side (ex: 192.168.1.1).

2) The device registers locally to the CNG SIP-IMS proxy (Registrar) using its local SIP URI. SIP REGISTER message is sent by the CNG to the NGN with the IMPU of the CNG which maps to the CND local SIP URI.

3) So as to allow the device to communicate through the NGN, the customer can configure the association between the local SIP URI of the device (pre-configured in the device) and the CNG's public IMS identity (IMPU), or the device can use its own public SIP URI (pre-configured in the device) to send the register through the CNG SIP proxy.

The authentication is handled directly by the CNG-SIP proxy B2BUA.

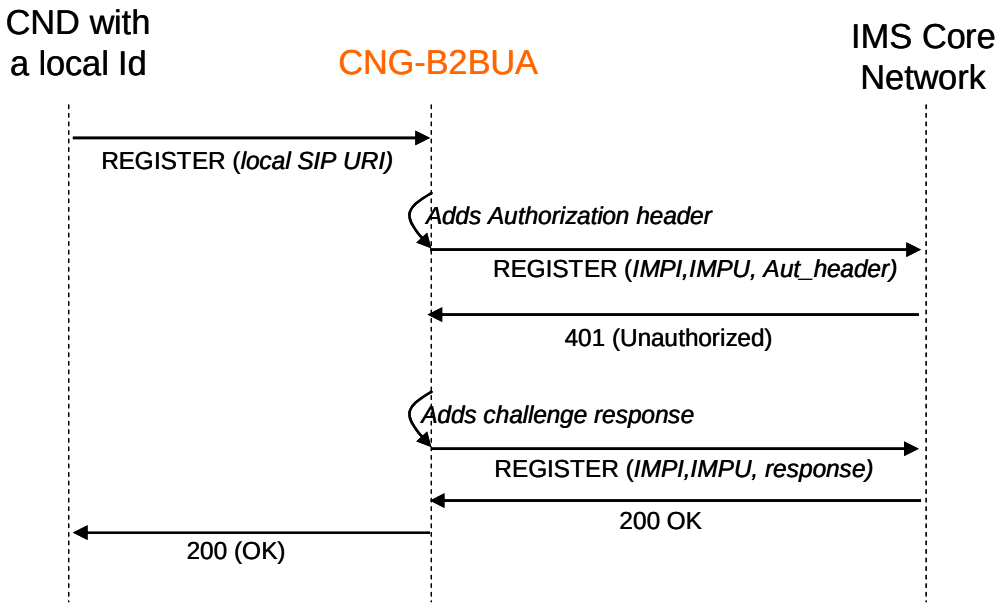


Figure 7: Non-IMS capable CND attachment and local/IMS registration

Other devices shall use their own IMPU (pre-configured in the device) to send the register directly to the NGN proxy. This should also be done through the CNG SIP proxy. It should be the case for instance for a nomadic device which should be able to register locally at the CNG level as it could use the option 120 not to know its registrar already provisioned, but to discover the outbound proxy within the CNG. This would give the opportunity for an IMS device to be involved in local SIP communications managed through the CNG SIP Proxy (e.g. call transfer). This case is described in figure 8.

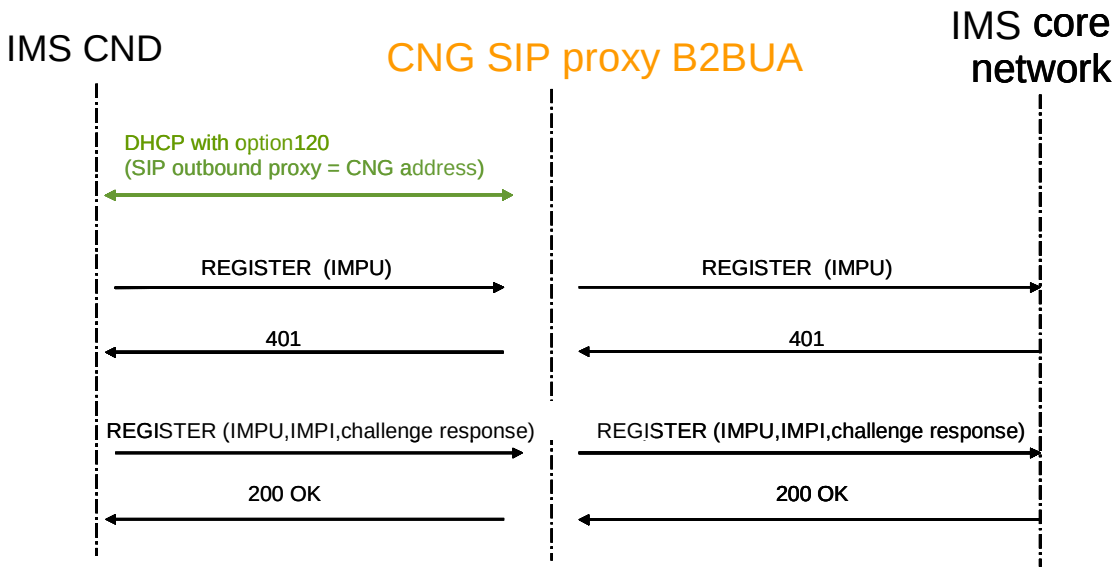


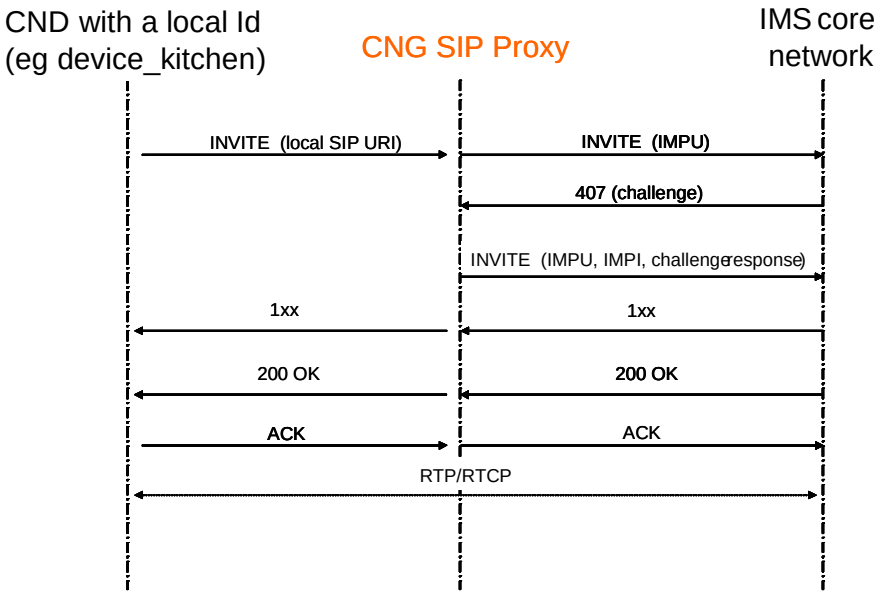
Figure 8: IMS capable CND attachment and IMS registration

NOTE: This scenario is not possible in case of IMS device implementing the AKA authentication mechanisms (IPsec tunnel through the CNG).

7.3.2 Outgoing call

7.3.2.1 SIP non-IMS CND

The SIP non-IMS device is provided with a public SIP URI or a local identity, as is the case in figure 9.

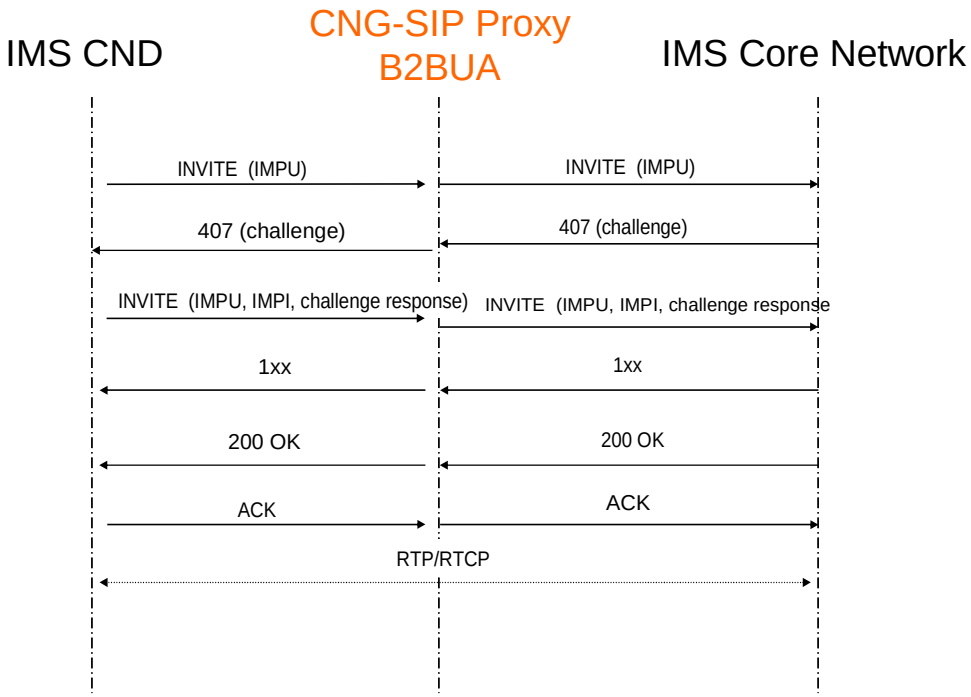


NOTE: The 407 (challenge) is optional.

Figure 9: Outgoing call for a non-IMS CND

For SIP non-IMS CND, the CNG SIP proxy can replace the device local SIP URI with its own IMPU in the SIP INVITE, in case the CNG IMPU is associated with several CNDs (only one register is sent to the P-CSCF for several devices with the same tel number).

7.3.2.2 IMS CND



NOTE: The 407 (challenge) is optional.

Figure 10: Outgoing call for a IMS CND

7.3.3 Internal call

The CNG SIP proxy can route local call between two devices of the CPN.

No NGN resource is used to establish internal call.

SIP signalling is not forwarded to core network and media streams are kept on the CPN directly between endpoints.

The SIP proxy identifies internal call after the analysis of the called party number.

The customer can dial:

a) Directly the local identity of the device (ex: kitchen, dect, John, etc.).

b) Or a private numbering plan. The commutation table is configurable for instance by the customer on the web server of the CNG.

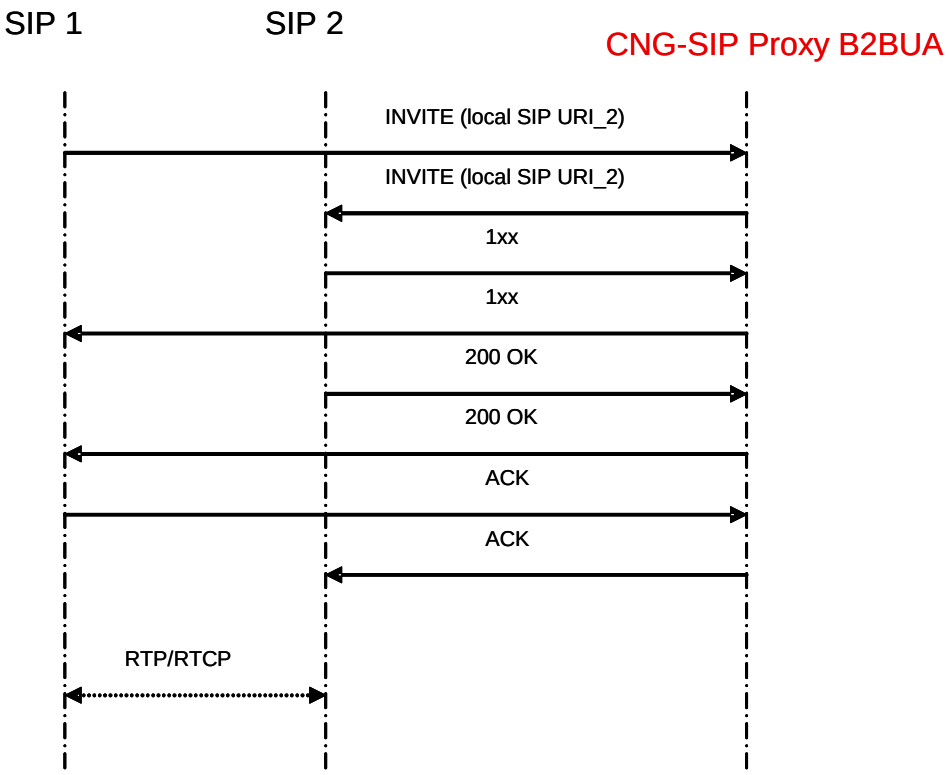


Figure 11: Internal call

7.3.4 Admission Control

The CNG-Admission Control Function (CNG-ACF) module calculates the available resources on the access line during the establishment of a new session, possibly limiting the number of sessions in advance, before the direct intervention of the RACS on the NGN side. As it has no means of reading signalling protocols other than unencrypted SIP, the result of this calculation may be wrong for the access line because of an underestimation of the total number of sessions. Still RACS will assure the proper result for the connection admission control over the access line and limit the session setup [i.7].

The module is considered as optional (as G_m' and G_m interfaces related to the SIP proxy).

The objective is to guaranty the quality of service for each new session and existing sessions previously established.

The B2BUA extracts from SIP message the SDP offer and announced capabilities (codec audio, video, etc.).

It asks to the CNG-ACF if announced capabilities are compliant with the available resource.

The CNG-ACF module returns 3 responses:

a) OK:

   a) The resource is available for all announced codecs.

   b) The initial SIP message is forwarded without any change on SDP part.

b) OK with restriction:

a) The initial SIP message is modified (incompatible codecs are suppressed from SDP part) and then forwarded.

b) The session can be established with an acceptable codec for network resource.

c) Not OK:

a) The B2BUA rejects the session establishment.

NOTE: The SIP profiles can be different from one side of the B2BUA to another.

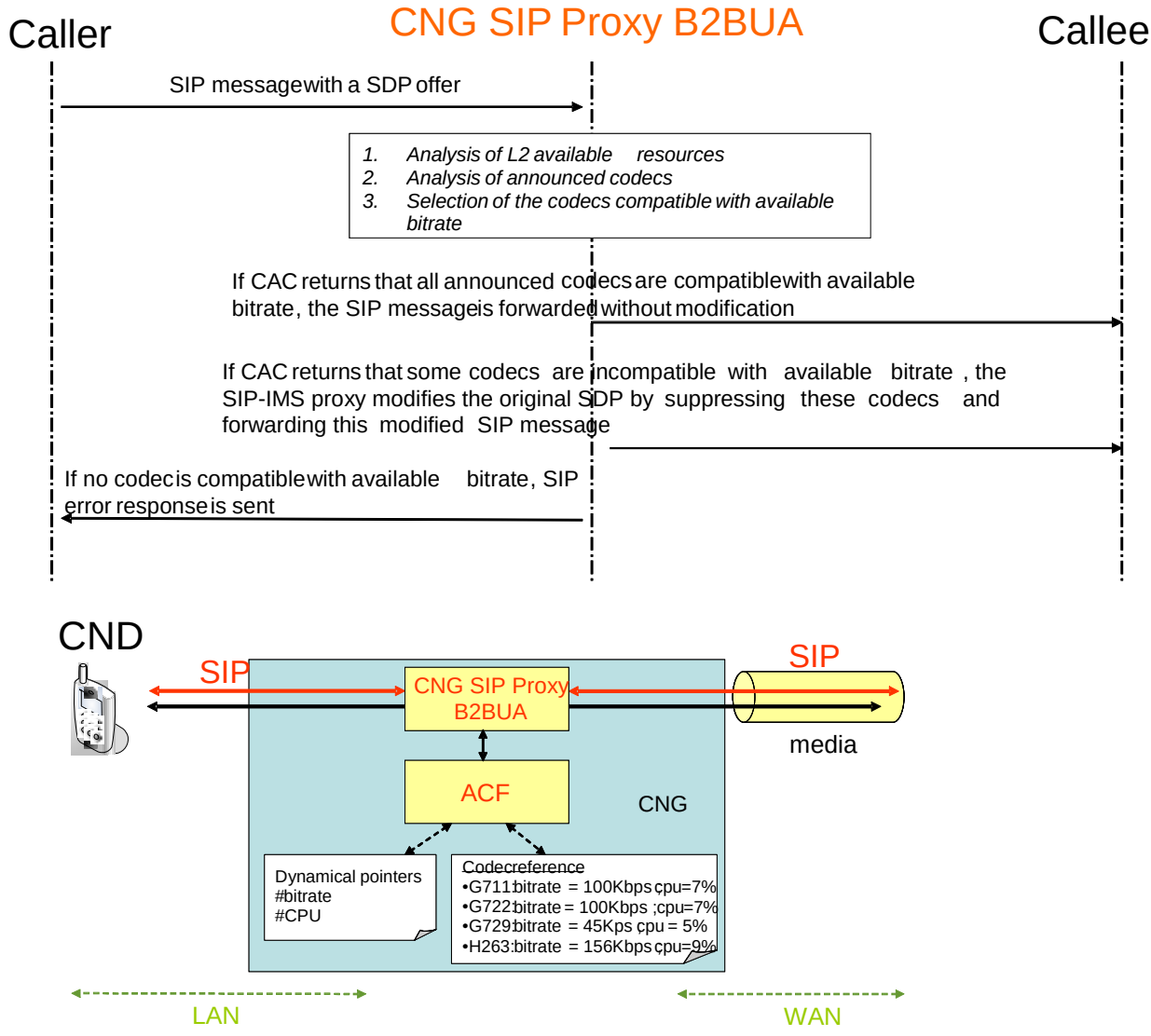


Figure 12: Admission Control within the CNG

7.4 Remote Access flows

7.4.1 Remote Access Connection Set-up

This clause describes one procedure where information of which CND's are registered in the CNG and therefore accessible via Remote Access, is retrieved by the remote UE. The UE provides an application linking the procedures for Remote Access services.

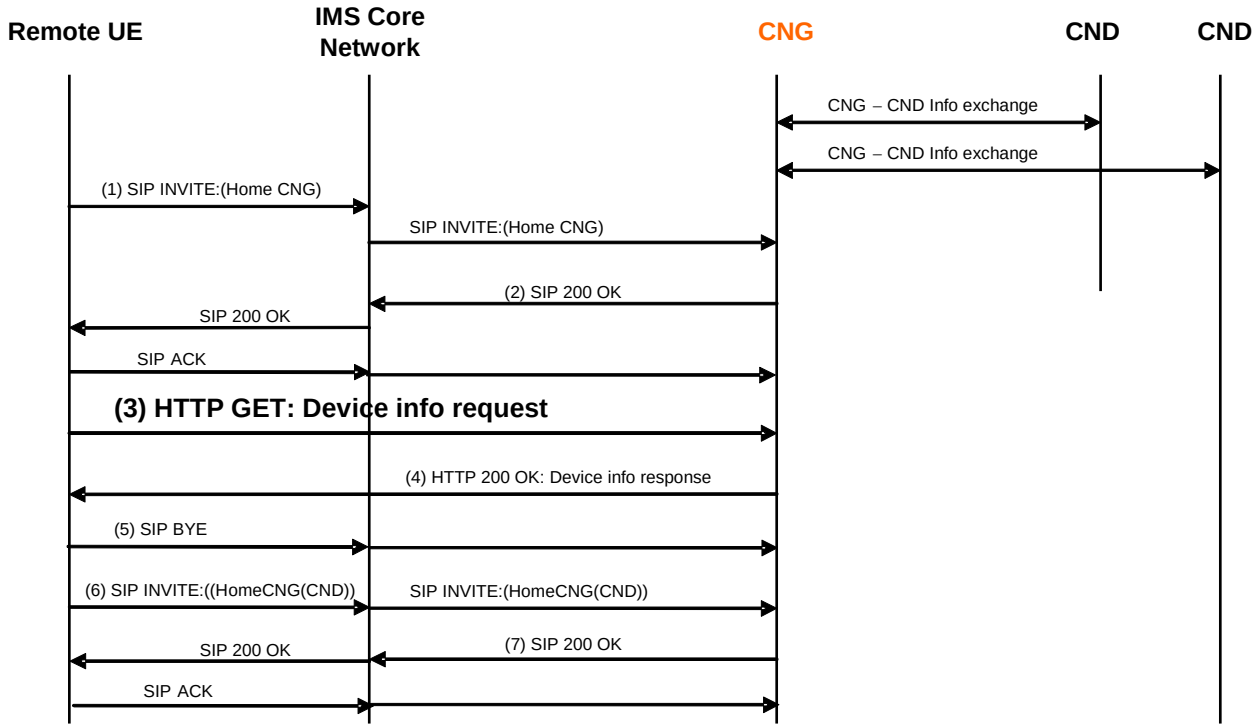


Figure 13: Remote Access Connection Setup

Prerequisite, the CND in the CPN has to be registered (e.g. using UPnP or similar procedure) to the CNG before the following take place:

1) The remote access menu initiates SIP INVITE to the users home CNG. The request is granted by the IMS NW and sent to CNG.

2) CNG checks if the request shall be granted. It initiates mapping of addresses and ports and prepares for the remote access procedures by returning SIP 200 OK.

Optionally a secure tunnel is then setup between the remote UE and the CNG.

3) HTTP GET carries (e.g. DLNA or similar procedure) requesting CND information including device types and identities to be provided.

4) CNG checks its present CND registrations, DB info (e.g. DLNA or similar) and returns the CND's device type, identity and pointer to CND in HTTP 200 OK.

5) This session is terminated with SIP BYE.

The Remote UE now holds the list of available CND's, their identities and types. The end user chooses the CND of interest and initiates a new session according to the following.

6) SIP INVITE is now sent addressing the CND (in the SDP part). The request is granted by the IMS NW and sent to the CNG.

7) CNG checks if the request shall be granted. It initiates mapping of addresses and ports and prepares for the remote access procedures by returning SIP 200 OK. Optionally a secure tunnel is then setup between the remote UE and the CNG.

NOTE: This initiated session will be terminated (SIP BYE) in the end of the sequence.

7.4.2 Download of content using HTTP

This clause describes the procedure where content is downloaded from a particular CND to the remote UE. The information about which CND's are available has been retrieved during the connection setup procedure. The UE provides an application linking the procedures for Remote Access services.

Prerequisite is the RA Connection set-up procedure displayed in clause 7.4.1:

1) The Remote UE points out the CND of interest using the path descriptor received under point 4 in clause 7.3.1.

2) CND sends an acknowledgement back to the Remote UE also indicating where to retrieve additional info.

3) The Remote UE sends a request (e.g. UPnP or similar) to the CND for additional device and service information.

4) CND responds with information about the services supported in the device.

5) The Remote UE browses the directories (e.g. with UPnP or similar procedure) where available content for download are located and makes a choice.

6) CND is responding with information (e.g. UPnP or similar) about the content URL/URI.

7) The Remote UE requests the download of data by addressing the content URL/URI.

8) The particular file is downloaded to the UE.

9) The connection is terminated with SIP BYE tearing down the session initiated by SIP INVITE in RA Connection setup described in clause 7.3.1, point 6.

In case of consecutive download requests the first four steps do not need to be repeated if the CND device and service information is cached in the Remote UE.

In the following flows the HTTP protocol is shown as an example although other alternative choices could be considered.

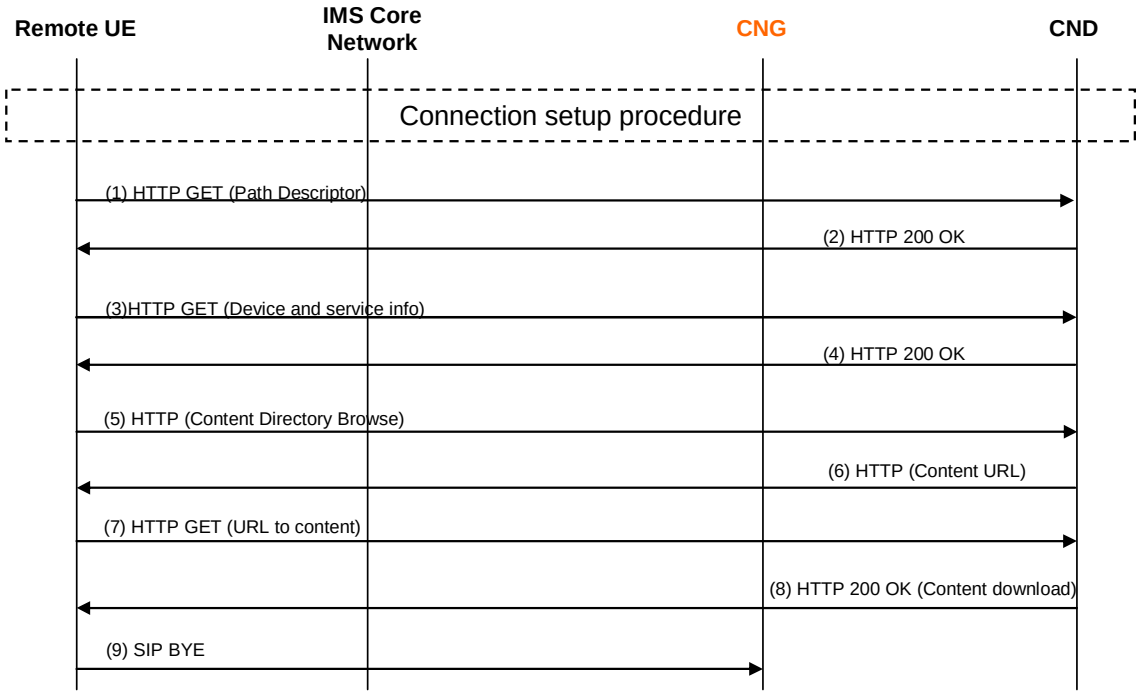


Figure 14: Download of content using HTTP

7.4.3 Upload of content using HTTP

This clause describes the procedure where content is uploaded to a particular CND from the remote UE. The information about which CND's are available has been retrieved during the connection setup procedure. The UE provides an application linking the procedures for Remote Access services.

Prerequisite is the RA Connection Setup procedure in clause 7.4.1:

1) The Remote UE points out the CND of interest using the path descriptor received under point 4 in clause 7.3.1.

2) CND sends an acknowledgement back to the Remote UE also indicating where to retrieve additional information.

3) The Remote UE sends a request (e.g. UPnP or similar) to the CND for additional device and service information.

4) CND responds with information about the services supported in the device.

5) The Remote UE browses the directories where content can be uploaded.

6) CND is responding with information about the content directory URL/URI.

7) The user selects the folder where content will be uploaded. An object is created for the pending file.

8) The Object description and URL/URI address is received by Remote UE.

9) The particular file (object) is uploaded to the CND.

10) CND is acknowledging the upload of content.

11) Disconnection is initiated with SIP BYE terminating the session initiated by SIP INVITE in RA Connection setup described in clause 7.3.1, point 6.

In case of consecutive upload requests the first four steps do not need to be repeated if the CND device and service information is cached in the Remote UE .

In the following flows the HTTP protocol is shown as an example although other alternative choices could be considered.

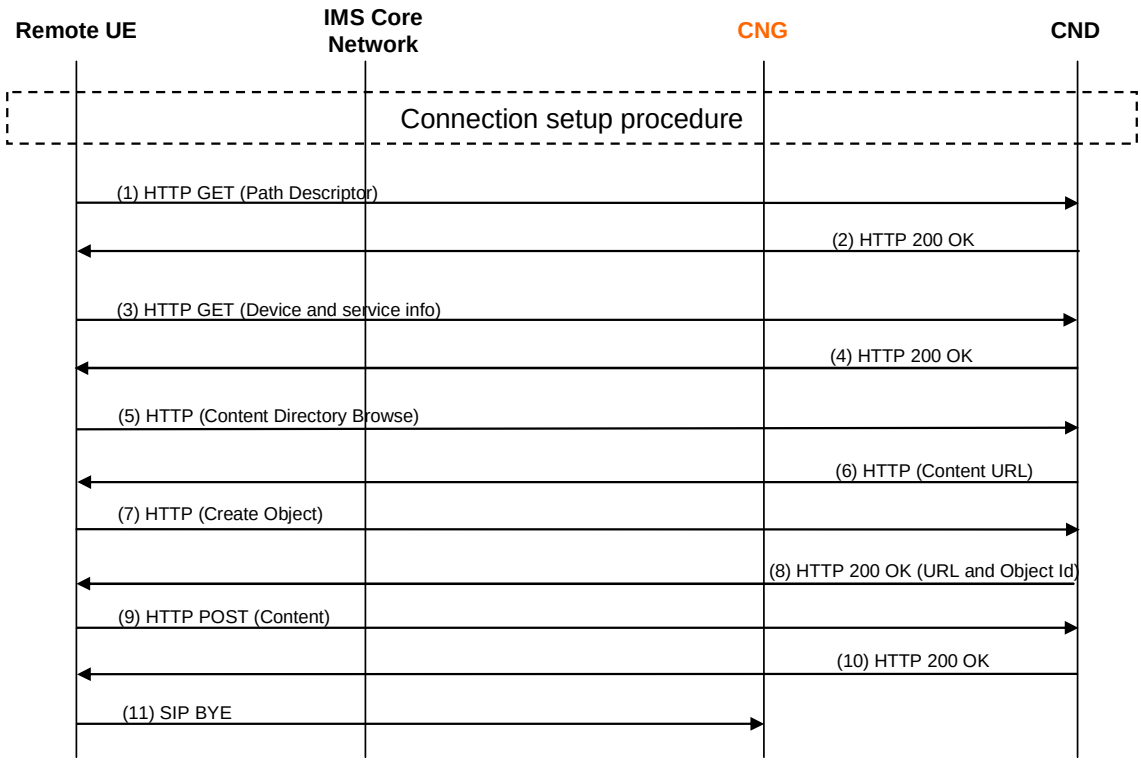


Figure 15: Upload of content using HTTP

Annex A (informative): Bibliography

ETSI TR 180 000: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Terminology".

HGI Forum specifications.

IETF NAPT traversal Working Groups: BEHAVE for STUN TURN methods, MMUSIC for ICE, SIP for SIP Outbound.

Annex B (informative): Change History

Date	WG Doc.	CR	Rev	CAT	Title / Comment	Current Version	New Version
06-05-08	WG5-02-008	001	1	F	Clarification on CNG Admission Control Function	2.0.0	2.0.1
06-05-08	WG5-02-009	002	1	F	Clarification on CNG Communication Services Media Function	2.0.0	2.0.1
06-05-08	WG5-02-010	003		F	Clarification on SIP Multi-mode	2.0.0	2.0.1
06-05-08	WG5-02-013	004	1	F	Early deployment IMS signalling path through CNG-Proxy B2BUA	2.0.0	2.0.1
02-07-08	18WTD119	005	1	F	Correction of the RA setup signalling flows	2.0.1	2.0.2
02-07-08	18WTD233	006	1	D	Clarifications in relation to Remote Access concerning RADA and RATA	2.0.1	2.0.2
02-07-08	18WTD336	007		D	Clarification in specification due to comments from HGI	2.0.1	2.0.2
11-07-08					All CRs approved at TISPAN#18	2.0.2	2.1.1
26-09-08	18bTD323	008	1	D	CNG – HGI Alignment	2.1.1	2.1.2
07-11-08					All CRs approved at TISPAN#19	2.1.2	2.2.1
22-01-09	19tTD223R1	009	1	F	Dj' reference point between the IPTV CND and the CNG	2.2.1	2.2.2
					Publication	2.2.2	2.3.1

History

Document history		
V2.0.0	March 2008	Publication
V2.3.1	June 2009	Publication