



Home Gateway Initiative

HGI guideline paper

HGI-GD006-R2
IMS Enabled HG

29/05/2009

PAGE LEFT INTENTIONALLY BLANK

Table of Contents

Table of Contents	4
1 Introduction - IMS Enabled HG	6
1.1 Outline of this document.....	6
1.2 IMS HG in HGI-RD001-R2	6
1.3 IMS standardization in 3GPP and TISPAN	7
2 Use Case: IMS enabled home	8
3 The NGN-IMS Architecture	10
3.1 The TISPAN NGN-IMS architecture.....	10
3.1.1 NGN Service Layer (IMS).....	12
3.1.2 NGN Transport Layer	12
3.1.2.1 NGN Transport Control Plane	13
3.1.2.2 NGN Transfer Function Plane.....	13
3.2 CNG in NGN-IMS architecture	14
3.2.1 The CND device	16
3.2.2 The CNG home gateway.....	16
3.2.3 The Access Network	16
3.2.4 The Core Network	17
3.3 NGN Network Mobility	17
4 IMS Enablers	18
4.1 IMS User Identities	18
4.1.1 IMS Subscriptions	18
4.1.2 IMS Identities in a IMS Enabled HG.....	19
4.1.3 Registration of IMPUs in IMS	19
4.1.4 Registration of Service Capabilities in IMS	20
4.2 IMS Security Architecture.....	20
4.2.1 Architecture for a non-IMS Enabled HG.....	22
4.3 Service Mobility and Roaming.....	23
4.4 SIP extensions for IMS.....	23
4.5 Standardized IMS Services.....	24
4.5.1 Standardized IMS Services for our Use Case.....	26
5 IMS capabilities in HGI-RD001-R2	27
6 IMS Enabled HG architectural description	29
6.1 IMS Interworking block.....	30
6.1.1 The Back-to-Back User Agent (B2BUA)	31
6.1.2 The WAN side SIP/IMS UA.....	32
6.1.3 SIP Server	33
6.1.4 ISIM/IMC.....	33
6.2 Interworking with the HG Resource and Admission Control Subsystem (G-RACS).....	33
6.2.1 NA(P)T and Firewall control functions.....	34
6.2.2 QoS handling and CAC	34
6.3 Signalling to LAN side SIP UAs	35
6.4 NASS related control functions in IMS Enabled HG	35
6.5 Configuration and management.....	36
6.5.1 CWMP (TR-069) based management.....	36
6.5.2 XCAP based management.....	36
6.5.3 Identity management block	37
6.5.4 Device management block.....	37
6.5.5 LM Remote UI block.....	37
7 Home device interworking with IMS HG	38
7.1 Non-IP devices	38
7.1.1 Special case: Analogue Terminal Adapter = ATA.....	38
7.1.2 Other adapters supported by HGI-RD001-R2.....	38
7.2 IP devices (non-SIP, non-IMS).....	39
7.3 IP devices (SIP enabled).....	39

7.4	IP devices (IMS/SIP enabled)	39
8	References	40
9	Acronyms	42
10	Definitions	47
10.1	Definitions from HGI-RD001-R2	47
10.2	Other Definitions used in this document	47
11	Important notice, IPR statement, disclaimer and copyright	49
12	Appendix	50
12.1	IMS based Remote Access	50

1 Introduction - IMS Enabled HG

This document, “IMS Enabled HG” (HGI-GD006-R2), provides additional explanation for the IMS requirements defined in the HGI Residential Profile, (HGI-RD001-R2) (HGI Residential Profile V. 1.0) [1]. It presents the IMS enabled HG (IMS HG) functions and behaviours, as well as the interaction with the NGN-IMS network and with home devices.

IMS enablers that have been included in HGI-RD001-R2, such as user identities, charging and authentication framework enable managed IMS based services like VoIP, IPTV and RA to be delivered to the home. The IMS HG also supports delivery of IMS services to standard CE industry home devices.

This document, by providing a big-picture view of the IMS HG within the IMS architecture, is meant to make the requirements contained in HG-RD001-R2 easier to understand, for both service providers looking at deploying the IMS enabled HG, and for vendors needing to understand the HG requirements.

1.1 Outline of this document

Chapters 1-4 contain informative information around the IMS enabled HG, while chapters 5-7 provides specific guidance to the IMS HG requirements as defined in HGI-RD001-R2.

Informative part to an IMS Enabled HG (chapter 1-4):

- Introduction and references to standardization activities in TISPAN and 3GPP
- A Use Case for an IMS enabled home, including personalized IMS services for conversed telephony, IPTV and Remote Access.
- Description over the IMS enabled HG in the NGN-IMS architecture (TISPAN).
- The most important IMS Enablers are described (IMS User Identities, IMS Security Architecture, Service Mobility and Roaming, SIP extensions for IMS and Standardized IMS Services)

Guidelines for an IMS Enabled HG as defined in HGI-RD001-R2 (chapter 5-7):

- Description and references to IMS parts in IMS HG in HGI-RD001-R2 .
- Enhanced HG architectural description over the IMS interworking part, including references to requirements in HGI-RD001-R2 .
- An improved IMS HG architecture figure (Figure 13) with LAN and WAN interfaces in line with TISPAN.
- Home Devices interworking with the IMS enabled HG.

1.2 IMS HG in HGI-RD001-R2

HGI-RD001-R2 [1] lists requirements for an HG system. A number of these requirements fit into the NGN-IMS architecture as described by ETSI TISPAN. In particular with regard to IMS capability, this IMS enabled HG system supports;

- Network connectivity for IMS devices
- The HG system acting as an IMS proxy for non-IMS home devices.

The IMS capabilities and architecture fit into a broader NGN network context. Both NGN and IMS network and capabilities are described in a set of ETSI TISPAN documents.

The NGN capability assumes a digital Ethernet/IP based network. In fact, almost all HGI-RD001-R2 specification requirements are NGN capabilities.

In addition, the IMS capability presumes SIP based signalling, IMS based user/device identification and authentication, secure communication, and mobility. This guideline document focuses on these HG specific IMS capabilities. The specific IMS related requirements from HGI-RD001-R2 are listed in chapter 5.

1.3 IMS standardization in 3GPP and TISPAN

This section helps the reader to understand the different versions of IMS and explains which versions are aligned with the HGI work. Essentially, the reader should know that HGI work is aligned as closely as possible with ETSI TISPAN WG5 (TISPAN R2). IMS functionalities up to 3GPP release 7 are reflected in this document, one exception is the authentication framework (including IMC definition) that is from 3GPP release 8 [8].

Internet protocol Multimedia Subsystem (IMS) is defined as a global, access-independent and standard-based IP connectivity and service control architecture that enables various types of multimedia services to end-users using common Internet-based protocols [8, 17]. It is one of the possible service layer platforms included in the overall Next Generation Network (NGN) architecture considered by ETSI, together with the PES (PSTN/ISDN Emulation Subsystem) and IPTV (non-IMS based). The NGN as defined by ETSI, is described in ES 282 001 and the integration of the IMS within this architecture is specified in ES 282 007.

Previously IMS was standardized in both 3GPP and in TISPAN organizations. From July 2007 on, the overall responsibility for the evolution of the IMS platform has been assigned to 3GPP, while future TISPAN activities will refer to the “Common IMS” platform resulting from a merge of 3GPP and TISPAN specifications. The 3GPP R8 version of TS 24.229 is the first document that provides IMS standardization in one “Common IMS” document. The IMS platform evolution was earlier specified in 3GPP TS 24.229 (R7) (for mobile) and in TS 24.503 (additions for fixed) [35].

ETSI TISPAN WG5 has finalised the R2 specifications in the home for support of NGN as defined in ES 282 001 [12] and in ES 282 007 [31]. ETSI TISPAN R2 is aligned towards 3GPP Release 7. The most relevant documents for TISPAN R2 are: (CNG corresponds to IMS HG and CND to HD)

- CNG technical stage 2 specification TS 185 003 [14]
- Interfaces to CNG in technical report TR 185 007 [16].
- CND in technical stage 2 specification TS 185 006 [15].
- ETSI TS 185 010 [34] is the ETSI TISPAN R2 Customer Premises Protocol specification that will replace the TR 185 007 [16]

TISPAN procedure is to develop Stage 1, 2 and 3 specifications; which corresponds to service requirements (Stage 1), functional architecture and procedure description (Stage 2) and protocol specification (Stage 3).

2 Use Case: IMS enabled home

One Use Case (UC), as an example, is described in this section in order to better understand the IMS enabled HG and its interaction to home devices and users. The UC is focusing on the usage of fixed and mobile telephones in the home.

We are in Mr. Martin's home containing a home gateway as described in HGI-RD001-R2 specification [1]. The family consists of Dad, Mom and the children Bob and Nancy. Mr. Martin (as the head of the family) has selected a set of services in a subscription from his BSP:

- Mr. Martin has subscribed to have a family telephone number, meaning that all users in the home can be reached at this family phone number (functions as a traditional "black" phone)
- Mr. Martin has also selected to have personal telephone numbers coupled to each user in the family. This service is configurable by Mr. Martin. Nancy is too young to have her own phone number.
- Mr. Martin has Remote Access (RA) capabilities included in the subscription, meaning that he remotely can access the home from remote using his (Dad) mobile phone.
- Dad has a mobile phone subscription from the BSP.

Mr. Martin's family lives in a house and have subscribed to a broadband subscription from his BSP in his area. Within the home there are Ethernet (100MBit/s) cables to all rooms and a wireless connection (Wi-Fi) is used from the mobile phones to the IMS HG. The devices that Mr. Martin has at home are summarized below:

- A HGI IMS HG with a IMS-subscription from the BSP and having FXS ports for POTS and wireless capabilities (Wi-Fi or DECT)
- Two old POTS telephones connected to the FXS ports of the IMS HG, whereof one is dedicated to the Family and one to Dad.
- Three SIP telephones connected to the IMS HG via Ethernet (or Wi-Fi). One of the phones is dedicated to Bob, and the other two can be used by Mom, Dad or Bob respectively.
- Dad has an IMS enabled mobile phone with a subscription from his BSP, including ISIM and Wi-Fi against the IMS HG.
- Mom has an advanced pre-paid mobile phone, with a subscription from ASP1 (non IMS subscription). This mobile phone has SIP capabilities and can connect to the IMS HG using Wi-Fi.
- An IPTV system that consists of a flat screen connected to a STB. An IPTV subscription is part of the offer from the BSP, associated with the IMS HG.
- Two PCs, one dedicated to Dad and one to be used by the whole family (Dad, Mom or Bob).
- A DLNA certified Media Server where the family stores photos and films.

From this UC we can conclude that from an IMS perspective (that works with Users) different types of home devices exist in Mr. Martins home. A first differentiation is:

- Devices statically configured to one User: Dad's IMS mobile phone, Dad's PC and Dad's POTS phone. Mom has her mobile phone. Bob has a SIP phone. The Family has a POTS phone, IPTV system and Media Server.
- Devices dynamically allocated to Users: The "Family PC" and the "Family phones" do not belong to any specific User in Mr. Martins home before authentication. As an example Bob can use the "Family PC" log in using his credential against the IMS HG. After a successful authentication the "Family PC" now is registered in IMS with Bob as a user. Bob can now use the PC to get his IMS services also to this device. It can be noted that those devices that can "dynamically" be allocated to any User in the home, need to have some type of

“GUI” so that each user can be authenticated against the IMS HG. Note: The IPTV system could also be dynamically allocated to a User (or Users).

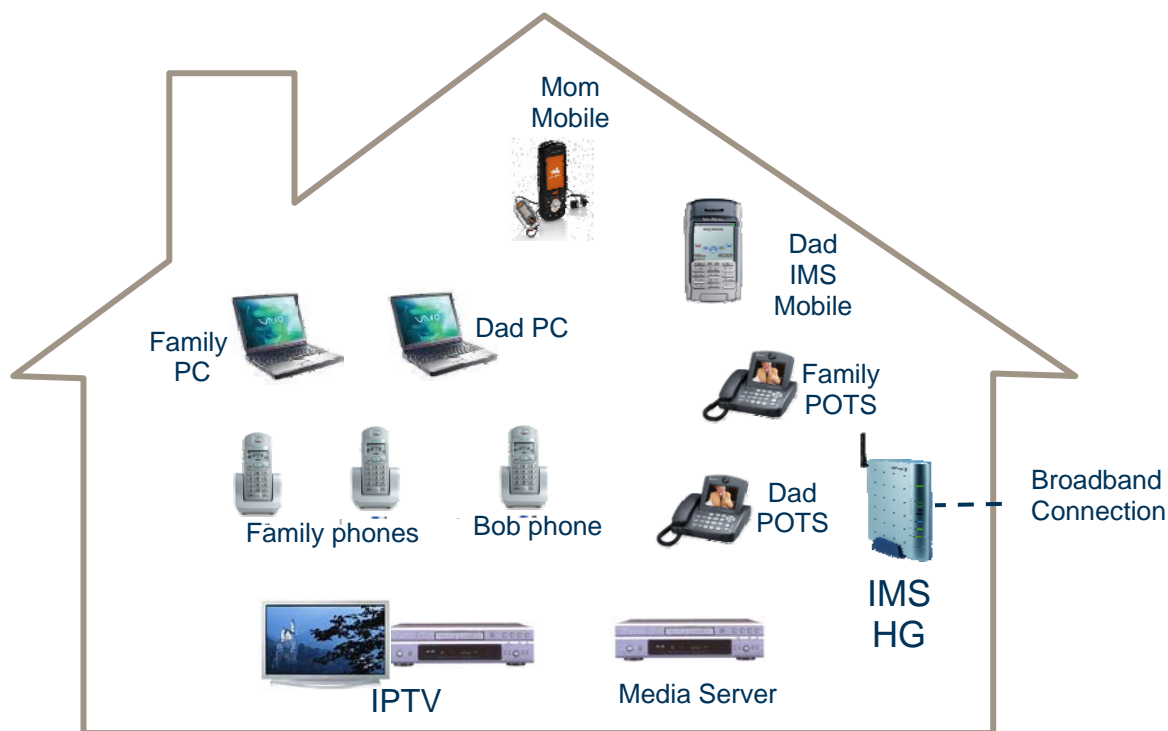


Figure 1 Overview of devices in Mr. Martin's house

There are two IMS enabled devices inside Mr. Martin's home, Dad's Mobile phone and the IMS HG. The IMS HG acts as an identity proxy for those devices that do not have the capability to connect to IMS (not IMS enabled devices).

Example of IMS standardized services described in section 4.5 (in this Guideline document) that can be used in Mr. Martin's house are:

- MM Telephony: Mr. Martin's home subscription includes a family phone number, as well as personalized telephone numbers for each family member in Mr. Martin's home.
- Personalized IPTV service based on IMS.
- IMS based Remote Access service allows Mr. Martin's phone to access photos and films from outside the home.
- When any of the persons in Mr. Martin's family is registered in IMS, the Presence and Messaging services can be used.

3 The NGN-IMS Architecture

The NGN network, including the Internet protocol Multimedia Subsystem (IMS), is defined as a global, access-independent and standard-based IP connectivity and service control architecture. It enables various types of multimedia services to end-users using the IP protocol for transfer. The information taken from TISPAN in this chapter is based on TISPAN R2 documents only.

The NGN-IMS network architecture is shown in ETSI document ES 282 001 [12], which:

- Structures the NGN/IMS architecture in NGN layers (not to be confused with OSI layers). This is kind of horizontal layering of functions.
- Shows functional entities in each of the layers and reference points on interfaces between entities and their naming.
- Shows however the Devices (called User Equipment) as single blocks, have interfaces to the different NGN layers, but does not show home gateway explicitly.
- Does not describe very well where the functional entities are located in the network (access network, core network).

Complementary to this, documents ETSI TS 185 003 [14] and TS 185 006 [15] respectively elaborate on functional entities in the home gateway (CNG) and the device (CND).

This chapter starts with a section (3.1) that gives an overview of TISPAN NGN layers and main functional entities as presented in ES 282 001 [12]. In a second section (3.2), NGN layers are extended into the CNG and the CND with a focus on the CNG in the NGN-IMS architecture. This architecture also positions the different functional entities in CND, CNG, Access network and/or Core network. This is kind of a vertical layering. In a last section the mobility aspect for devices is considered in the NGN network. Visiting (guest access) devices may connect over a HG to the HG's access network, which will proxy requests to the visiting device's home network (mobile-context).

It must be noted that the functional entities used from ES 282 001 [12], are limited to those dealing with home gateway functionalities. For instance, all functional entities related to Media Gateway communication are left out.

3.1 The TISPAN NGN-IMS architecture

This section presents the following figure (Figure 2) which is composed based on:

- NGN functional architecture (ES 282 001 [12]) including the NGN layering and Transport layer functional entities.
- IMS functional architecture (ES 282 007 [31]) and Service layer entities.
- The NASS functional architecture (ES 282 004 [13]) and its entities.
- The RACS functional architecture (ES 282 003 [32]) and its entities.

Figure 2 presents the TISPAN functional entities into one single architecture diagram which is NGN layer based. This figure does not show the functional entities of the User Equipment yet, nor does it show the vertical NGN layering. The TISPAN NGN-IMS layered architecture is as follows:

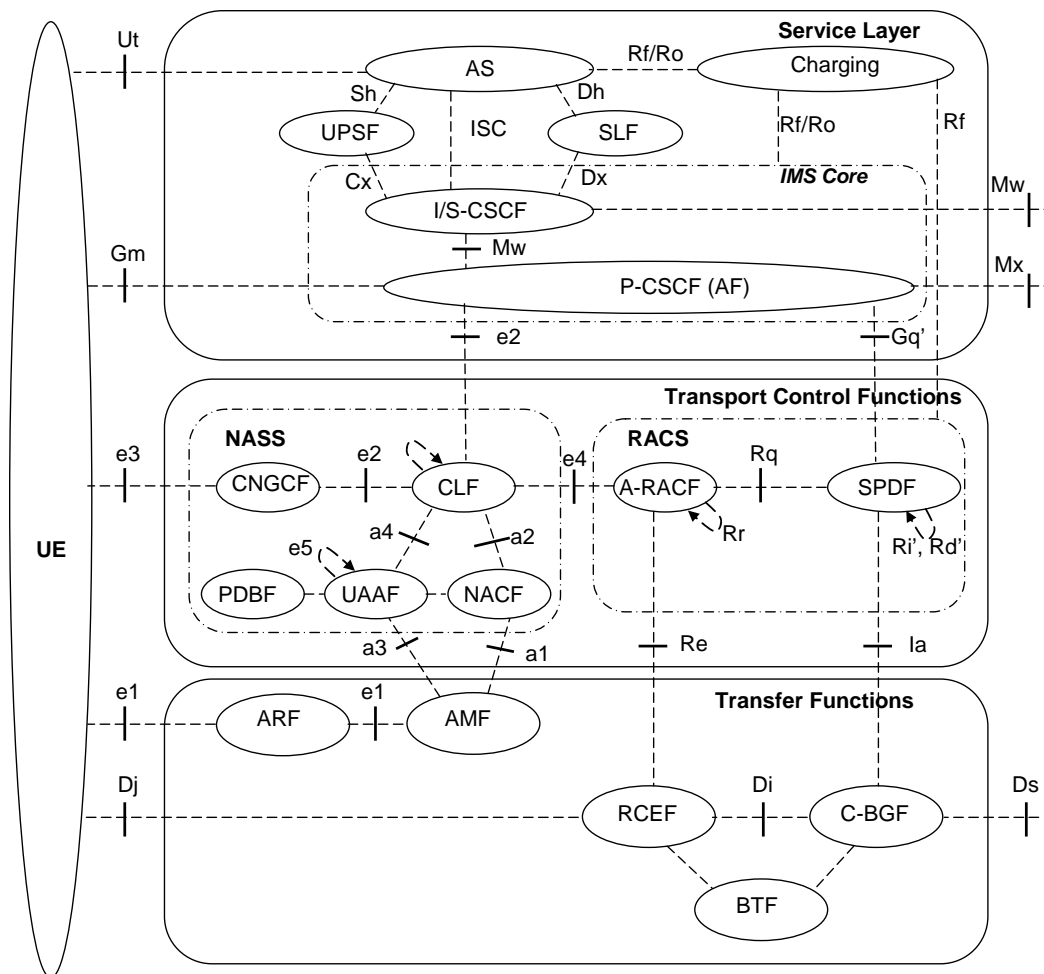


Figure 2 TISPAN NGN-IMS architecture: Layers and main blocks

The TISPAN NGN-IMS network functions are categorized (horizontal classification) in so-called NGN layers (not to be confused with OSI layers):

- **The NGN Service layer**
This represents functions related to signalling, services, applications and charging functions.
- **The NGN Transport layer**
This represents access and resource control functions, as well as data transfer.
 - **The Transport control plane**
Access and resource control functions, including the NASS and RACS functions.
 - **The Transfer functions plane**
Coding, enforcing and transfer functions, including direct control on data transfer like address translation, firewalling, queuing, flow control, error correction, and more.

The User Equipment (UE) in TISPAN and its interfaces is both applicable to end devices (CND) and home gateways (CNG). The ES 282 001 [12] document states that UE contains both CND and CNG. In the TS 185 xxx series of ETSI specifications, the functions inside the CND and CNG are presented.

The following subsections explain the different functional entities shown in Figure 2.

3.1.1 NGN Service Layer (IMS)

The NGN Service Layer consists of the IMS Core and Application Servers (AS). The IMS Core consists of a large number of nodes, whereof the CSCF and UPSF and Application Servers (AS) are explained below. From the NGN Service Layer there are two reference points defined against the UE (also applicable for the IMS enabled HG); the **Ut** and the **Gm**. Over the Gm interface, the control signalling between the IMS Terminal and the CSCF takes place. The Ut interface is an interface over which the service configuration can be communicated.

- **Call Session Control Function (CSCF)**, composed by three different entities; Proxy (P-CSCF), Serving and Interrogating. Common to all CSCFs is that they play a role during registration and session establishment and for the SIP routing mechanisms. Moreover, all functions are able to send charging data. Both proxy and serving CSCFs are able to release sessions on behalf of the user (hanging sessions, lost bearers), and to check the SDP content to verify whether it contains media types or codecs, which are not allowed for a user. When the proposed SDP doesn't fit the operator's policy, the CSCF rejects the request and sends a SIP error message to the user.

Specifically, the S-CSCF authenticates the user (on the service layer, using the registrar server functionalities), In case of successful authentication the P-CSCF establishes a secure association with the IMS terminal (or IMS HG). This association may take the form of an IP association, a TLS session or an IPSec Security Association (SA) A P-CSCF can also compress/decompress SIP messages to reduce the round-trip over slow links. The standard allows the use of NASS-IMS Bundled authentication and HTTP Digest as authentication methods for those IMS terminals (or IMS HG) where IMS AKA cannot be used [8]. The P-CSCF is assigned to an IMS terminal during registration, and does not change during the registration. Other nodes trust the P-CSCF, and do not have to authenticate the user again. Further the P-CSCF plays a role in the network admission control communicating with the RACS.

- **Subscription Locator Function (SLF)** is used by the Application Server (AS) and the CSCF to retrieve the address of the User Profile Server Function (UPSF) which holds the subscription data for a given user (not needed if there is only one UPSF).
- **User Profile Server Function (UPSF)** (equivalent to a Home Subscriber Server (HSS) without the HLR portion) is the database where user data is stored. The HSS is responsible for generating keys and challenges. For instance, in case of IMS AKA, the long-term key on the UE side is implemented in the ISIM module (implemented on a UICC). In the case IMS AKA is not applicable, the IMC module stores the related credentials (e.g. for HTTP Digest). The HSS is the network function storing the same set of credentials associated with the IMPI. The subscriber will have at least one IMPI and one IMPU.
- **AS**, is the **Application Server** that is connected to IMS. It can, for example, be a VoIP or IPTV application server. See separate section on standardized IMS services.

Within the core network, a number of reference points are identified in Figure 2: Mx, Mw, Cx, ISC, Dx, Dh and Sh.

3.1.2 NGN Transport Layer

The NGN IP Transport Layer consists of the Transfer Functions (also called Transport Processing) plane and the Transport Control plane. The Transport Control plane deals with network connectivity and resource control. The NGN Transport Control plane is interfacing the NGN Service Layer. The Transfer plane deals with transfer of data over the network and directly related control functions (address translation, firewalling etc.)

3.1.2.1 NGN Transport Control Plane

The NGN Transport Control Plane is interfacing the NGN Service Layer (containing IMS Core, Application Servers, and Service Control Subsystems) via the e2 and Gq' interface.

The NGN Transport Control plane in the Access and Core network is divided into two main functions; the RACS and the NASS as shown in Figure 2. They are connected via the e4 interface.

Resource Admission Control Subsystem (RACS) is based on the Service Policy Decision Function (SPDF) which is a logical policy decision element for service-based policy control, and the Resource Admission Control Function (RACF), dealing with the admission of new sessions taking into account available network resources. SPDF and RACF are communicating via the Rq interface.

The RACS interfaces in the network with the Transfer Function plane are via reference points Re and the Ia reference point respectively for the RACF and the SPDF functions. The SPDF interfaces with the P-CSCF (also called Application Function (AF)) via the Gq' interface. There is no interface between the UE and the RACS.

Network Attachment SubSystem (NASS), supports the dynamic provisioning of IP address and other user equipment configuration parameters (e.g. using DHCP). NASS supports User (or HG) authentication to access network, authorization of network access and access network configuration (based on user profile), and location management. Two authentication types are considered for network access: implicit authentication (based on access identity like the line identification) and explicit authentication (using an authentication protocol). It is a matter of operator policy whether implicit or explicit authentication is applied.

The sub-functions inside the NASS are:

- **User Access Authorization Function (UAAF)**, performing user authentication, as well as authorization checking, based on user profiles, for network access. For each user, the UAAF retrieves authentication data and access authorization information from the user network profile information contained in the Profile Data Base Function (PDBF).
- **Network Access Configuration Function (NACF)**, responsible for the IP address allocation to the UE and distribution of network configuration parameters such as address of DNS server(s), proxies, DHCP servers etc. Note that the NACF corresponds to the DHCP Server in HGI-RD001-R2 specification [1].
- **CNG Configuration Function (CNGCF)**, used during initialization and update of the CNG (IMS HG). The CNGCF provides additional management configuration information to the CNG (IMS HG). Example of configuration is firewall internally and QoS marking of IP packets. The CNGCF in TISPAN terminology corresponds to TR-069 ACS in HGI-RD001-R2 specification [1].
- **Connectivity session Location and repository Function (CLF)** registers the association between the IP address, the network location information provided by NACF (e.g. the line identifier), the geographical location, and the user information as provided by the UAAF. The function responds to location queries from the P-CSCF.

The interface between the UE and the NASS (CNGCF function) is represented by the e3 reference point.

3.1.2.2 NGN Transfer Function Plane

The NGN Transfer Function plane consists of a number of blocks that interact with the RACS and NASS sub-systems in the Transport Control plane. The UE interacts with the Transfer Function Plane (RCEF) over the Dj reference point. Inside the NGN Transfer Function plane there

are blocks that are related to the control data transfer, and blocks that are responsible for the user data transfer.

The reference point for the control data transfer is e1. The blocks for the control data transfer against the NASS sub-systems are (see Figure 2):

- Access Relay Function (ARF) acts as a signalling relay between the user equipment and the Network Attachment Subsystem (NASS). It receives network access requests from the user equipment and forwards them to the NASS. Before forwarding a request, the ARF may also insert local configuration information and apply protocol conversion procedures.
- Access Management Function (AMF) acts as an entry point for the NASS, distributing requests to the appropriate functions (e.g. UAAF or NACF).

The reference point for the data transfer is Dj. The blocks are (see Figure 2):

- The Resource Enforcement Control Function (RCEF) acts basically as an enforcement point when entering the access network (kind of a firewall function in the access network).
- The (Core) Border Gateway Function (C-BGF) acts basically as an enforcement point when entering the core network.
- The Bearer Transport Function (BTF) acts as a forwarding function for data/media information.

3.2 CNG in NGN-IMS architecture

In Figure 2, functional entities are located somewhere within the horizontal layering. The following important information is not shown in Figure 2:

- A vertical positioning of functions: are they located in the access network, in the core network, or in both?
- The distinction between CND and CNG
- The corresponding NGN-IMS functions in the CND and CNG, and their position in the horizontal layering. Quite some info can be obtained from the TISPAN TS 185 xxx documents.

Figure 3 is produced by HGI to clarify the NGN-IMS architecture. The figure specifically shows how the CNG fits into the NGN-IMS architecture. The figure is based on the TISPAN NGN-IMS architecture, but in addition separates CND and CNG, extends the horizontal layers into CNG and CND, positions the functional entities in CNG and CND in corresponding NGN-IMS blocks, and categorizes the network functions also vertically. As such, some blocks in the figure do not 'strictly' correspond to the ones defined in TISPAN, although the alignment is kept as close as possible. But the added value in Figure 3 is that it gives a global view on the NGN-IMS fixed network access architecture, while it also leaves out the media gateway (control), which is less applicable in HGI.

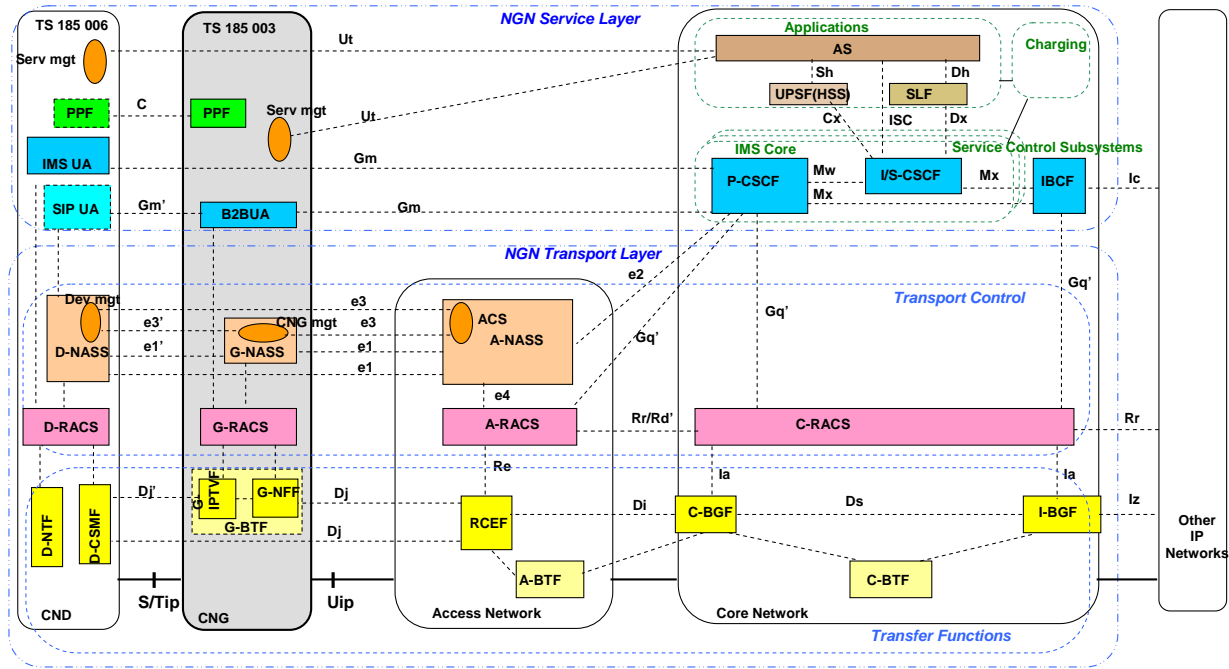


Figure 3 Overview of the NGN-IMS architecture, showing the CNG interactions

The NGN-IMS network functions are categorized (vertical classification) in functional entities classified according to the location related to the network: device (CND), home gateway (CNG), access network, and core network. Reference points on physical interconnections are S/T (between CND and CNG) and U (between CNG and IP-based network). The ip index refers to the NGN being an IP based network. The other reference points indicated are on logical (non-physical) interfaces between functionalities.

Figure 3 extends the NGN layers up to the device (CND) and the home gateway (CNG), as an integral part of the NGN-IMS network. Note that also this figure, like Figure 2, does not include the NGN-IMS entities related to media gateways (MGW, MGCF, etc.) because the HGI-RD001-R2 specification [1] does not support this.

Figure 3 uses different colours for application (brown), service signalling (blue), access control and configuration/management (orange), resource control (magenta), and transfer (yellow). Details in Figure 3 are limited to the main blocks (transfer blocks, NASS, RACS, signalling and application management blocks). A deeper view of the sub-functions in the CNG (IMS HG) is given in chapter 6. The functional entities for CND and CNG shown in the figure are based on information in TS 185 006 [15] and TS 185 003 [14] respectively, although Figure 3 better emphasises the NGN-IMS horizontal layering and related functions.

Looking at the NGN layers in the Figure 3, it is shown that the main functions of NGN, reappear in the CND and CNG:

- Application functions.
- Signalling functions (User Agents UA, CSCF): different names are applied in the different vertical classification blocks.
- NASS functions: the prefix indicates the vertical block: D-, G-, and A-NASS for respectively Device, Gateway, and Access network.
- RACS functions: the prefix indicates the vertical block: D-, G-, A- and C-NASS for respectively Device, Gateway, Access network and Core network.
- Enforcement functions and transfer functions.

3.2.1 The CND device

The CND considered here is either IMS enabled or SIP non-IMS enabled (a TA may be needed). In the first case the CND contains an IMS User Agent function and in the second case it just contains a SIP UA function (not using any IMS credentials). The call related communication for an IMS enabled CND is transparent through the CNG, then the Gm interface is used. For a SIP non-IMS enabled CND, the call related communication is through the B2BUA in the CNG, then the Gm' interface is used.

A CND device contains a D-NASS function, allowing connectivity and management functions. CND gets its IP address from a DHCP server in CNG or in NASS and is managed with CWMP protocol. Via the Ut interface IMS services can be managed by the end user, and the PPF function inside the CND can be used to detect other home devices.

A CND contains a D-RACS function, providing local admission control and resource control. There is no communication of the RACS function to any other RACS entity.

The device also contains a data termination function called Communication Services Media Function (D-CSMF). This is the function terminating the media flows by providing an appropriate codec. The NAPT Transversal function D-NTF allows application flows to traverse a NAPT enabled CNG, e.g. by using STUN based binding between the CND SIPUA and P-CSCF.

3.2.2 The CNG home gateway

An IMS enabled CNG includes an IMS B2BUA with an IMS security module either being the ISIM or IMC module, with which it can identify itself to the IMS network, using a private identity. Further it acts as an IMS enabler for non-IMS devices in the LAN, using public identities identifying these devices towards the IMS network .

A CNG contains a G-NASS function, allowing WAN access connectivity and management, including network authentication, IP address allocation (via DHCP or PPP) and network management (via CWMP). Towards the LAN devices, the CNG includes a DHCP server for private IP address allocation.

A CNG contains a G-RACS function, providing local admission control and resource control. There is no communication of the G-RACS function to any other RACS entities outside CNG.

The CNG also contains a data transfer function called the Gateway Bearer Transfer Function G-BTF (HGI additional function to TISPAN). It includes the NAPT and Firewall function (G-NFF), which conforms to the RCEF and BTF functions. TISPAN has also included an IPTV function in G-BTF. This IPTV function (G-IPTVF) is included in Figure 3.

3.2.3 The Access Network

The access network contains the A-NASS as explained in section 3.1.2.1 and the A-RACS function. The A-RACS may communicate to other x-RACS functions (example C-RACS) either in the same domain or in other domains. The A-RACS contains the functions RACF and SPDF. The transport layer functions in the Access Network are RCEF and A-BTF.

3.2.4 The Core Network

The core network contains NGN service layer functions as explained in section 3.1.1. The core network does not contain a NASS function. The RACS function in the core network is the C-RACS that contains the functions RACF and SPDF. The transport layer functions in the Core Network are C-BGF and IBGF as enforcement functions, and C-BTF for data transfer.

3.3 NGN Network Mobility

The NGN architecture also supports Network Mobility which means that an NGN user can connect to a Visited Access Network using his own subscription valid in his Home Access Network. The NGN users need to authenticate against his Home Network. Therefore some blocks in the Visited Access Network need to relay the signalling. In particular the UAAF and the CLF (in the Visited Access Network), are acting as proxy servers in order to connect to the appropriate servers in the Home Access Network. Note that there is no proxy for the PDBF, since this is accessed over the UAAF. Detailed procedures are described in ETSI 282 004 [13].

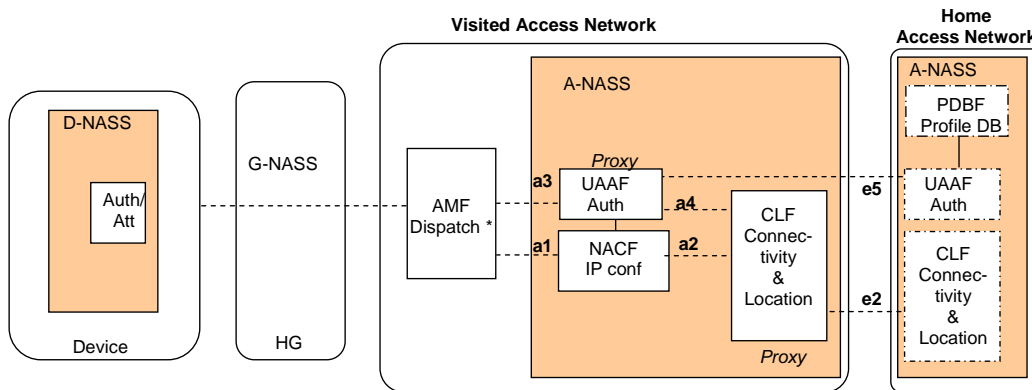


Figure 4 NGN Network Mobility architecture including Device and HG [13]

The G-NASS in the HG gets its WAN IP address from the A-NASS. For a visiting device (guest) in the home, the HG typically needs to have a dedicated SSID for visitor (for Wi-Fi) as proposed in HGI-RD001-R2 specification [1]. The authentication methods used by the visitor against UAAF has many dependencies, one is the authentication protocol used [4].

4 IMS Enablers

4.1 IMS User Identities

An IMS terminal (end device or IMS HG) needs to have at least one private IMS identity (IMPI) and one public IMS identity (IMPU). The IMPI is connected to the user's subscription and is used for authentication purposes, and the IMPUs can be defined as the public addresses of the user in the IMS network for different sets of services. Both the IMPI and the IMPUs are implemented as SIP URIs (IMPU can also be a Telephone URI).

The Private user ID (IMPI) is a unique global identity defined by the home network operator. It may be used within the home network to uniquely identify the user from a network perspective and is used for authentication purposes. It does not identify the user himself; on the contrary, it identifies the IMS user's subscription. It is possible to utilize private user identities for accounting and administration purposes as well.

The Public user ID (IMPU) is the user identity in the IMS network. IMPUs are the identities used for requesting communication with other users. IMPUs can be published. The IMPU takes form of either a SIP URI [27] or a telephone URI [28] and is assigned by the home network operator. It will not be possible for the end user to modify the IMPU. The IMPI associated with the IMPU is authenticated by the network during registration and may be used to identify user's information within the user profile database (UPSF).

4.1.1 IMS Subscriptions

The IMS private and public identities can be combined into different end user subscriptions. Example of different combinations of IMPI, IMPU and Service Profile into an IMS subscription is provided in the figure below.

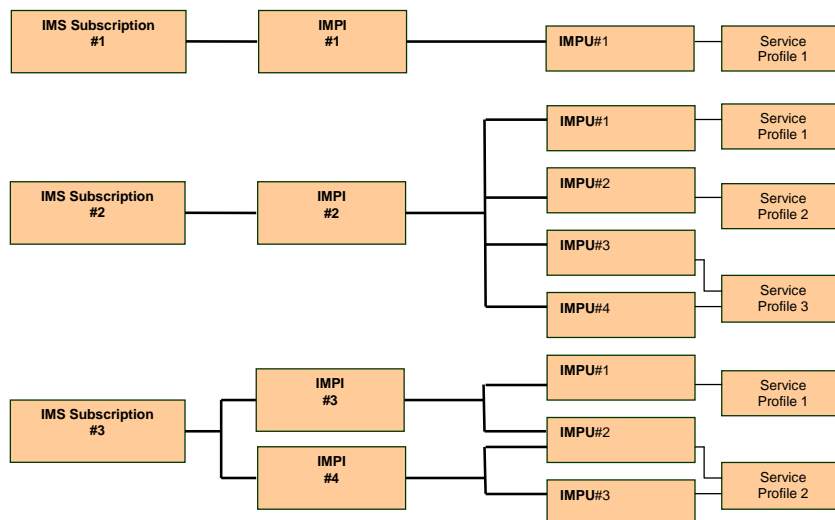


Figure 5 Examples of three different IMS subscription variants

IMS Subscription #1 is typical a mobile phone subscription that only requires one public identity (IMPU), while IMS Subscription #2 has a number of public identities and service profiles included in the subscription. Example of IMS Subscription #2 is the IMS enabled HG, where each family member in Mr. Martins Family has a public identity. IMS Subscription #3 shows the possibilities to have more than one IMPI (that each has a security association with IMS) in an IMS subscription. Example here is the offering from the BSP, including Dad's IMS Mobile and the IMS enabled HG in one subscription (as in our use case). From the IMS Subscription #3, we also see that the two IMPIs have a common IMPU. This means that the user having this public IMPU can be

reached at devices that have different IMPIs (both at the phone and in the home). More information about IMS Identities can be found in the 3GPP TS 23.228 document [17].

4.1.2 IMS Identities in a IMS Enabled HG

The IMS Identity structure in an IMS enabled HG is very much depending on what IMS services that Mr. Martin wants to subscribe to, and to the number of family members that need to have individual personalized services. Some basic concepts are explained below and shown in Figure 6.

- An ISIM or IMC application provides storage for a collection of information that is relevant to the IMS sub-system, including identity information. There is at least one private user identity and one or more public user identities.
- There is one HG subscription per physical household. It has an IMS private identity (IMPI). A household with multiple physical addresses will most likely have one home gateway per physical address and each home gateway will have a unique IMPI.
- In addition, each member of the family can have one or more dedicated IMS public identities (IMPUs) in IMS, to get personalized services. We here call this type of IMPUs for "User specific IMPUs". Example here are services to Dad's PC and POTS phone, where personalized services become active first after a successful authentication against the IMS HG and the explicit registration of Dad's IMPU(s) in IMS (done by IMS HG).

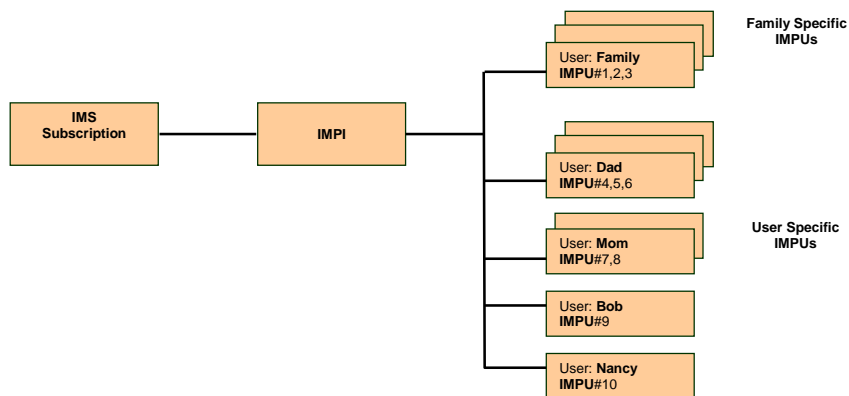


Figure 6 Examples of IMS identities in IMS enabled HG

4.1.3 Registration of IMPUs in IMS

Implicit registration is the mechanism by which an IMS enabled HG is allowed to register simultaneously to more than one of his/her IMPUs. The HSS knows the identities that are to be implicitly registered when it receives the indication of the registration of an individual identity. The notification of a registration of an IMPU implies the registration of the corresponding implicitly registered IMPU set. The user information downloaded in the response contains the IMPUs of the implicitly registered IMPU set with the associated service profiles. As an example from our use case is Dads IMPUs that are implicit registered when Dad has registered one of his IMPU, (for example when he starts using his PC and authenticates to the IMS HG).

4.1.4 Registration of Service Capabilities in IMS

When an IMPU is registered in IMS by the IMS HG, the IMS HG becomes the contact address for this IMPU. In this registration, the IMS HG can include the ICSI [17] feature tags, to indicate what IMS services capabilities that are supported by this IMPU (MMtel, IPTV etc.).

4.2 IMS Security Architecture

TISPAN/3GPP standards require for registration in IMS, the presence of an IMS authentication function including the long term credentials needed. The long term credentials can be provided in the IMS HG (or home device) either in an ISIM module or in an IMC module [8]:

- ISIM module: a common security module that can be used with any IMS access technology and the definition makes ISIM an application residing on a UICC. The security architecture of TISPAN/3GPP using ISIM provides mutual authentication between the NGN-UE and the NGN IMS core with the use of IMS AKA for authentication [10].
 - The ISIM module is preconfigured with all the necessary parameters to initiate the registration towards IMS. During the authentication process, Security Associations (SAs) are established between the NGN-UE (IMS terminal) and the P-CSCF (IMS core) to protect IMS flows. The SAs use the IPsec ESP protocol to provide integrity and if it is required confidentiality through the access network.
- IMC module: a common security module supporting those IMS terminals where IMS AKA cannot be used. The IMC module includes IMS security data and for IMS access. The IMC module is defined in 3GPP TR 21.905 [33] and authentication methods are specified in specified in 3GPP TS 24.229 [8].
 - Example of IMC authentication methods is the usage of a NASS IMS Bundled authentication and SIP based HTTP Digest authentication as defined in ETSI TS 187 003 [36]. These solutions exclude the need of an ISIM application on the UICC for authentication of IMS HG against IMS core. The ISIM application also includes other parameters (SIP, IMS identities etc.) that must be included in the IMC module.

The ISIM shall be used when authenticating towards IMS using IMS AKA. IMC shall be used when no ISIM is available, and should store the credentials for the relevant authentication method such as Digest authentication (if Digest authentication used).

The HSS (UPSF) in IMS Core is the database where user data is stored and is responsible for generating keys and challenges (see Figure 3). The long-term keys used for authentication is placed in the ISIM/IMC security module and in the HSS (UPSF) in IMS Core. This long-term key is associated with the IMPI.

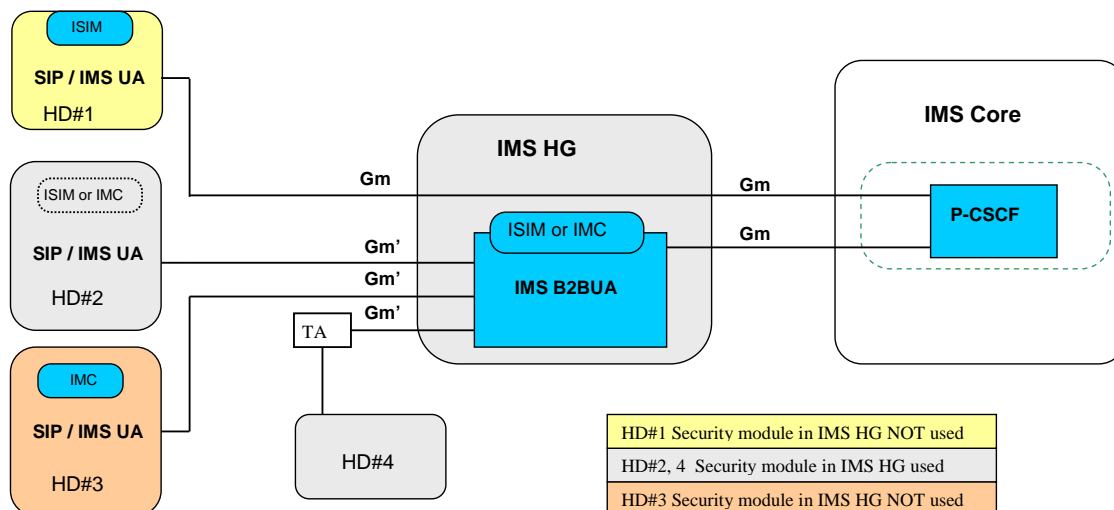


Figure 7 IMS security architecture overview for the home when using an IMS HG

Figure 7 shows the IMS security architecture including an IMS Enabled Home Gateway (IMS HG) and Home Devices (HD). The home devices have been categorized into 4 different groups HD#1, HD#2, HD#3 and HD#4. Below follow a description of how the IMS security is fulfilled for these 4 groups of home devices:

- HD#1: To this category belong those home devices that require the use of IMS AKA as authentication method against P-CSCF. A HD#1 home device must have an USIM or ISIM module that holds the long-term keys used for the IMS AKA authentication. When HD#1 type of devices require encrypted control-plane the IMS B2BUA in the IMS HG can not handle IMS Interworking for those devices.
 - The authentication signalling has to go transparently through the IMS HG (NAT and Firewall) over the Gm interface. A security association is established between the HD and IMS core. After a successful authentication the HD (User) is registered as active in IMS. If the HD does not have an ISIM application, but instead have an USIM application (example 3G phone), there are standardized ways how this USIM application can be used for IMS core authentication.
- HD#2: To this category belong those SIP/IMS home devices where the IMS Interworking block (IMS B2BUA) takes care of the interworking against IMS Core.
 - The long term secret in the ISIM or IMC module in the IMS HG is used when the IMS HG performs authentication and registration in IMS Core.
 - The HD#2 type of home device needs to be known by the IMS HG. LAN side authentication (e.g. Digest) toward the SIP registrar in the IMS HG might be required.
 - The IMS Interworking block can handle QoS, CAC and NAT traversal.
 - As indicated in Figure 7, those home devices can have an ISIM or IMC module for registration towards IMS. This security module is not used when the IMS HG takes care of the IMS security on behalf of HD#2 home devices.
- HD#3: To this category belong those SIP/IMS home devices that do NOT make use of ISIM or IMC security module in the IMS HG.
 - The long term secret in the IMC module is used towards IMS Core.
 - Home device might not be known by the IMS HG (can be a visitor)
 - The IMS B2BUA behaves as an “IMS Proxy” for the control signalling from the home devices towards the P-CSCF.
 - The IMS Interworking block can handle QoS, CAC and NAT traversal.
 - Example is an IMS Terminal using Digest authentication towards IMS Core.
- HD#4: To this category of home devices belong those that are controlled by the IMS interworking block in the IMS HG via an external or internal Terminal Adapter (TA). The IMS Interworking block takes care of the interworking with IMS Core.
 - The long term secret in the ISIM or IMC module in the IMS HG is used.
 - Examples of HD#4 type of home devices are legacy POTS phones, and OITF (STB) devices defined by Open IPTV Forum.

For an IMS enabled HG, the IMS Interworking block (IMS B2BUA) should “ideally” take care of the IMS interworking for all home devices. Then the IMS HG can perform QoS, CaC and NAT traversal functions. Local registration (in SIP Registrar in IMS HG) of home devices enables local calls as well as personalized IMS services.

The case when the HG is not IMS enabled (not including the IMS Interworking functions) The IMS terminals HD#1 as well as HD#3 can connect towards IMS Core over the Gm interface. HD#2 and HD#4 type of devices can for a non IMS enabled HG not get any IMS services.

4.2.1 Architecture for a non-IMS Enabled HG

Figure 8 below shows an example of how IMS home devices connects to the IMS Core via the HG. Note that the HD#2 and HD#4 type of home devices as defined in section 4.2 can not get access to IMS Services.

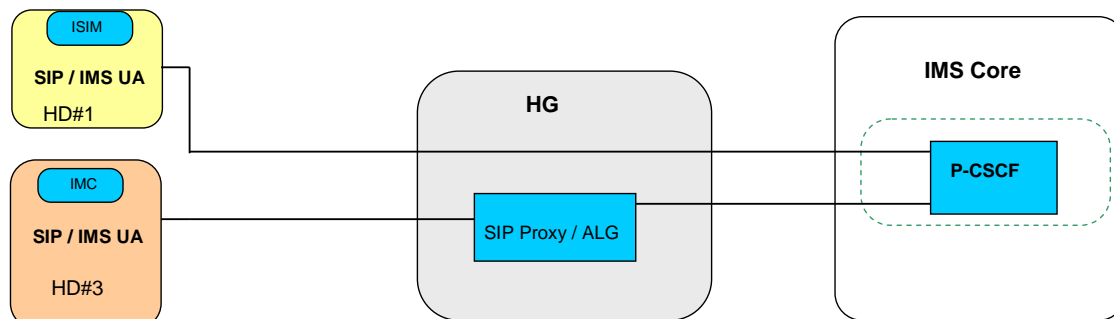


Figure 8 Example of home IMS devices connecting to IMS Core through HG

Like for an IMS Enabled HG (see Figure 7) the IMS device HD#1 has an ISIM security module and authenticates to IMS core using IMS AKA.

IMS device of type HD#3, having an IMC security module makes typical use of Digest authentication towards the P-CSCF. An HD #3 type device needs NAT traversal in the HG. A number of possibilities exist, Figure 8 shows the use of a SIP Proxy as specified in RFC3261 or use of a SIP ALG. An alternative to SIP Proxy/ALG in the HG is that HD#3 uses STUN for solving the NAT traversal through the HG.

4.3 Service Mobility and Roaming

Since IMS is originating from the mobile network environment, mobility is supported in the IMS network. Since HGI is considering fixed network access, service mobility is here restricted to a visitor having an IMS Terminal, for example a mobile phone (or the IMS HG itself). This means that the IMS User having an IMS Terminal can access his IMS-services from any location (home, at work, or as a Guest). One prerequisite is that the user IMS Terminal has network level information (IP address etc.) and to get this information the user need first register to the NASS [13].

Example of Service Mobility is the guest access feature as described in the HGI-RD001-R2 specification [1]. The Guest, having an IMS Terminal, connects to the IMS HG using Wi-Fi (using a separate SSID for guest access) and then performs authentication against IMS (P-CSCF) to get access to his IMS services from the visited home.

Once the guest has network access, he is able to communicate on application layer against IMS for enabling IMS services. This implies that he needs to register to a P-CSCF, where two alternatives exist:

- To the Proxy-CSCF in the visited network. Then SIP controlled communications happen, the IMS Terminal is using security associations and protection mechanisms in order to provide a secure communication. The ISIM-HSS provides for a mutual secured authentication, before any connection setup can take place. Detailed procedures are described in 3GPP TS33.203 [10]. Information about address to the P-CSCF can be obtained with use of DHCP Option 120 during the IP address assignment (see Figure 9).
- Directly to the Proxy-CSCF in the home network, based on information in the ISIM application in the IMS Terminal, (if no DHCP Option 120 information is present).

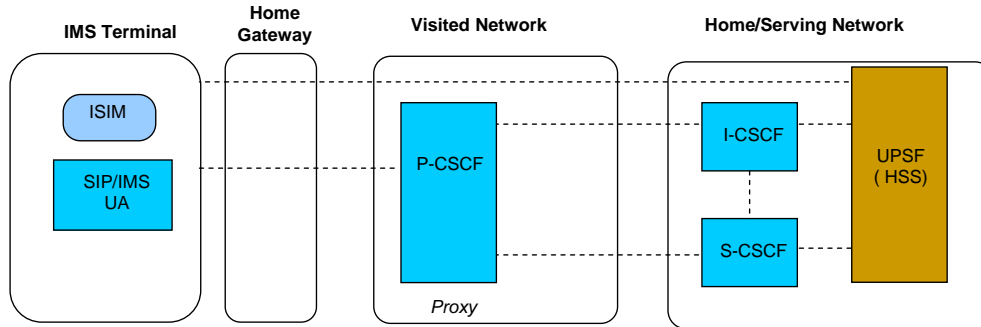


Figure 9 IMS authentication architecture for a visitor (IMS Terminal) against a P-CSCF in the visited network

Besides “Service Mobility” (access to services in the home network via the visited network) IMS also define “Roaming” scenarios between two IMS operators [26]. This means that a Guest (IMS user) in a visited IMS network can access IMS services in the visited network, without having a subscription with the visited IMS service provider. The two IMS service providers (home and visited) need to have a business agreement.

4.4 SIP extensions for IMS

SIP is a signalling protocol designed for controlling multimedia sessions and talented to replace previous voice and video signalling protocols like H.323 or the aged SS7. Standardized by the IETF [7], SIP supports different services from instant messaging to video conferences.

IMS, which makes use of SIP as its signalling protocol, has been presented as the framework able to provide a better service provisioning and control for mobile networks, but thanks to its independence from the access network, the IMS core has been adopted for the development of the NGN architecture. Standardized by the 3GPP, this evolved network architecture is intended to provide full multimedia control, resource and QoS end-to-end allocation, enhanced security, and to support new capabilities like FMC.

SIP provides IMS with its functionality as an application layer protocol that is used for establishing, modifying and terminating multimedia sessions in an IP network. Therefore SIP appears as the signalling protocol for managing multimedia sessions inside IMS. However, there are some key points that prevent the interoperability between a SIP client or server that fulfils the IETF specifications and an IMS terminal or network that follows the standards produced by 3GPP.

- 3GPP has developed its own specific SIP profile for IMS. This profile is known as the 3GPP SIP profile [8] and includes some special characteristics [9]:
- A greater number of compulsory messages. IMS flows include some messages which are not considered compulsory in the IETF specifications.
- A greater number of compulsory headers for each message. There is a large amount of SIP extensions that include new headers and some of these headers are compulsory in IMS flows.
- Private 3GPP headers. There are new headers specifically designed inside 3GPP. These headers (named P-Header) are used to provide different functionalities required by an IMS architecture that are not provided by any of the existing IETF headers.

The following flows are an example for a SIP/IMS call session between SIP/IMS UA and P-CSCF. The green flows are specific to IMS and are used for local resource reservation using the optional precondition mechanism.

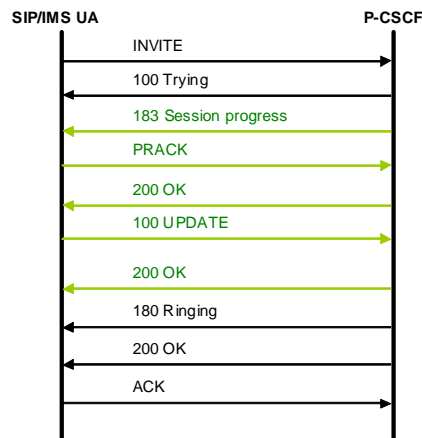


Figure 10 SIP/IMS session setup (including QoS precondition)

4.5 Standardized IMS Services

The IMS architecture allows for defining access-independent standard-based rich multimedia services. The base capabilities required for broadband and mobile services like charging, authentication, compression, routing, quality of service will be provided by the IMS Core and underlying sub-systems. IMS Services located in the application servers (AS), can via standardized interfaces (Ut and ISC) access these base capabilities of IMS. This allows for different standardization organizations, service providers and third party service providers to define new services in a standardized way reducing the time to market for new services.

The serving CSCF (Call Session Control Function) allocated to an IMS-user is the entity that determines the services that must be applied to the IMS-user and interfaces the application servers (AS). The interface between the serving CSCF (Call Session Control Function) and the application server is the SIP based ISC (IMS Service Control) interface.

Another interface to the application server is the Ut interface. This interface, between the IMS Terminal and the application server, allows manipulating various service related data such as the resource lists used for presence and push to talk. The Ut interface supports the HTTP-based XML Configuration Access Protocol. Other interfaces (see Figure 2) between the IMS core and the application server provide access to charging capabilities or the user data stored in the IMS database.

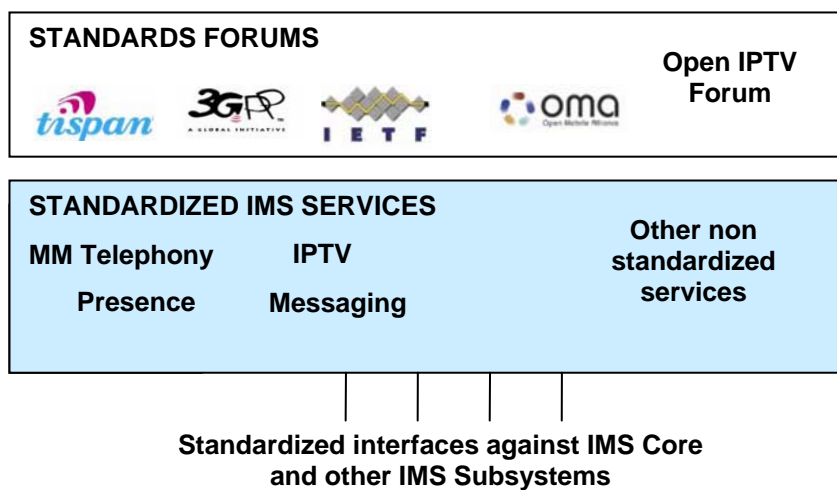


Figure 11 Overview of the main Standards Forums and the related Standardized IMS Services

As seen in the figure above, several organizations are working in the standardization of IMS services. Below is a summary of the most important:

- 3GPP has already standardized a multimedia telephony (MM Telephony) with supplementary services; furthermore it has also developed standards for messaging and presence [18-22].
- OMA (Open Mobile Alliance) also works in collaboration with 3GPP/3GPP2 to provide interoperable specifications of services integrating existing specifications when it is possible to reduce overlap. As an example, OMA has already created specifications for Presence and Messaging based on SIP SIMPLE (SIP SIMPLE defined by IETF) [23, 24].
- TISPAN forum is also actively involved in the standardization of services, using existing specifications when it is possible (Messaging or Presence services) and working in the definition of new services. There is ongoing work to standardize IPTV and RA services based on IMS and NGN network.
- Open IPTV Forum is another organization working in the standardization of a managed IPTV service based on IMS. Open IPTV Forum also defines a non-IMS IPTV solution [25].

The services mentioned above are only a brief overview of the standardization efforts that are being done by now. The aim of IMS is to be a framework for the development of new innovative services. These new innovative services, together with the standardized IMS-services, will enable the service provider to offer richer multimedia applications to the customers.

4.5.1 Standardized IMS Services for our Use Case

As described in our use case (in chapter 2), Mr. Martin has subscribed to have one or more public identity pointing to the household that are called "Family Specific IMPUs". Besides the "Family Specific IMPUs" each member of the family can have his dedicated "User Specific IMPUs". In this way personalized services can be provided for each member of the family. When the subscribing CSCF processes a request it evaluates the filter criteria defined in the database for the public identity provided and calls the services that must be applied. Below follows an example of how these standardized services can be applied to our use case in chapter 2.

- Mr. Martin's home subscription includes a family phone number, as well as personalized telephone numbers for each family member in Mr. Martins home. The MM Telephony standardized service has this telephone functionality.
- Mr. Martin Mobile phone subscription (from his BSP) includes convergence between fixed and mobile telephone systems. In this case, the MM Telephony service needs to interact with the mobile telephone system. This means that the standardized MM Telephony service needs to be extended with an application for that service [17].
- When any of the persons in Mr. Martin's family have registered against the IMS HG and the IMS User IMPU has been registered as active in IMS, the Presence of the user is then known by the IMS system. As an example, if Mom using the Family PC is registered in IMS, she can use the Presence service to get information about her friends.
- The Messaging services are subscribed to the users and allow them to send instant messaging (using pager messaging mode, analogous of SMS) or to chat with their friends (using session messaging mode) in an integrated environment.
- A Remote Access service allows Dad's phone to access personal photos and films from outside the home. IMS performs authentication and routing during the RA-setup of the phone from a remote location, to ensure a secure managed RA.
- Personalized IPTV service based on IMS.

5 IMS capabilities in HGI-RD001-R2

The HGI-RD001-R2 specification [1] describes the HG blocks and HG interaction with IMS in a number of places, where the most important are:

- Chapter 7, “HGI Reference architecture” specifies a number of IMS requirements, especially in section 7.1.11 (Fixed-Mobile and Service Convergence), section 7.1.15 (Messaging) and in section 7.1.10 (Security).
- Section 7.2, named “Moving towards a more IMS like architecture” describes why operators are interested in IMS type of architectures.
- Section 7.2.1 named “IMS-based remote access” describes a Remote access method where IMS is used to setup the media plane.
- The HG block diagram (Figure 5 in [1]) shows HGI architecture, including the Enablers for IMS; IMS and Identity handling-, Security- and Remote access blocks.
- IMS interworking sub-blocks and the connections against NGN network is shown in the IMS HG architecture Figure 12 below (corresponds to Figure 6 in HGI-RD001-R2 specification). A brief description of these sub-blocks can be found in section 7.5.2.

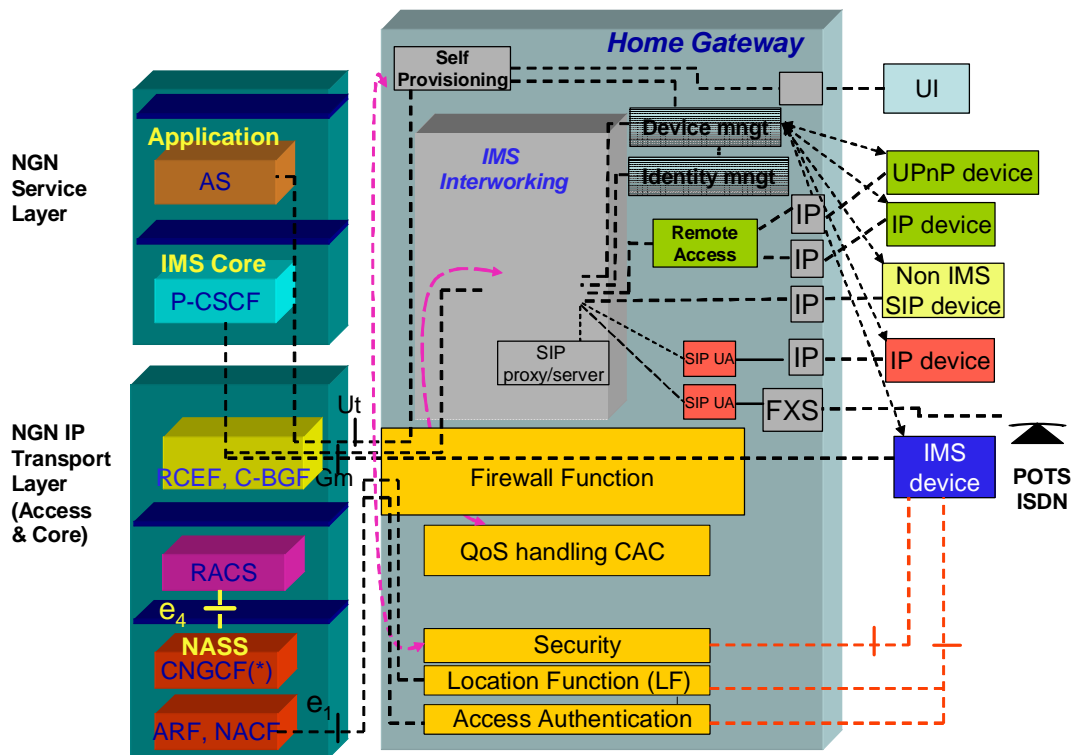


Figure 12 IMS HG Architecture figure, as shown in HGI-RD001-R2 [1]

When it comes to specific requirements for the IMS HG in HGI-RD001-R2 [1], they can mainly be found at the following places in HGI-RD001-R2 specification:

- Remote Access requirements for the IMS solution, can be found in section 8.7 in HGI-RD001-R2 specification. The Remote Access solutions defined in HGI-RD001-R2 have in detail been described in a separate HGI Guideline document named “Remote Access” [2].
 - Remote End-Device Access in section 8.7 (R235-R237).
 - IMS Approach in section 8.7.1.2 (R242-R246)
 - Remote Access Configuration and in section 8.7.2 (R247-R248).
- IMS communication service support requirements can be found in section 8.8.4, which has been divided into the following sub-sections:

-
- IMS Protocol Stack (IMS UA) requirements in section 8.8.4.1. (R269-R277)
 - IMS telephony user agent requirements in section 8.8.4.2. (R278-R284)
 - IMS Interworking with non-IMS home devices in section 8.8.4.3 (R285 to R287)
 - Local registration and local services support requirements in 8.8.4.4. (R288-R306)
 - Support of call forking in section 8.8.4.5. (R307-R308)
 - B2BUA requirements for CAC using SIP signalling in section 8.10.9.1 (R511-R517)

6 IMS Enabled HG architectural description

HGI-RD001-R2 specification [1] requires that the IMS HG and the home devices need to interoperate with the NGN core as defined by ETSI TISPAN, reference architecture detailed in ETSI ES 282 001[12]. In particular, the IMS functions in a home device and in the IMS HG should support IMS services based on the IMS platform as shown in Figure 2.

The IMS capability is much related to the fact whether the CPE (IMS HG or home devices) has an ISIM/IMC security module or not. The IMS HG must have an ISIM/IMC security module to be able to authenticate and register to the NGN/IMS network. It may be possible that the ISIM/IMC security module is replaceable depending on the IMS supporting service provider that is actually used. The ISIM security module with the needed IMS information is placed on an UICC card [30].

A general architecture showing the possible IMS enabled CPE's in the home in relation with the NGN-IMS network is given in Figure 7 and in Figure 12. Figure 7 shows the IMS security architecture for different type of home devices (HD#1-4), while the IMS HG Architecture Figure 12 (from HGI-RD001-R2) shows the different home devices connecting to the IMS HG.

It must be stressed that the NGN-IMS enabled HG (IMS HG) performs the interworking between the IMS Core and those home devices that are non-IMS or those IMS terminals that do not support IMS-AKA (not having an ISIM module). For the non-IMS terminals the IMS HG fulfils the typical IMS functions (like secure identification) on behalf of the non-IMS terminal in the home. For IMS terminals including an IMC security module, the IMS B2BUA in the IMS HG behaves as a proxy using the home device IMC module credentials. An IMS terminal in the home that has an ISIM module (and requires use of IMS AKA) needs to connect directly to the NGN/IMS network and not via the IMS Interworking block in IMS HG. The IMS interworking block can not handle encrypted control plane as required by IMS AKA. (See section 4.2 for more information)

The HGI-RD001-R2 specification [1] presents a general block diagram of the HG in its Figure 5, and a block diagram focused on IMS-NGN in its Figure 6 (Figure 12 in previous chapter). This section supports conceptually this figure, but elaborates it further in order to:

- Group functions into Management/Control/Data transfer, bringing it more in alignment with the general block diagram.
- Show much clearer the peer-to-peer relations, without grouping them through the firewall; it is evident that all communication has to pass through the firewall and lower layers.
- Add a number of additional peer-to-peer interfaces, conforming to the ETSI documents.
- Add a few more sub-blocks better showing the interaction with the IMS-NGN environment.

This leads to an improved (more detailed) NGN IMS-enabled home gateway block diagram. in the next figure, showing:

- A distinction between data transfer, control and management functions.
- Interfaces on the WAN side to the NGN-IMS functional blocks with which the HG has a direct communication.
- Interfaces on the LAN side to a number of different home device equipments, IP/SIP/UPnP enabled or not.
- Internal in IMS HG interfaces to included LAN side adapters.
- Particular interconnection(s) to an IMS enabled device(s), that is not only interfacing to the HG, but has direct communication (shown in red dashed lines) via the HG with some of the NGN-IMS functional blocks.

The different sub-blocks of the NGN-IMS Enabled HG are explained in the following sub-sections.

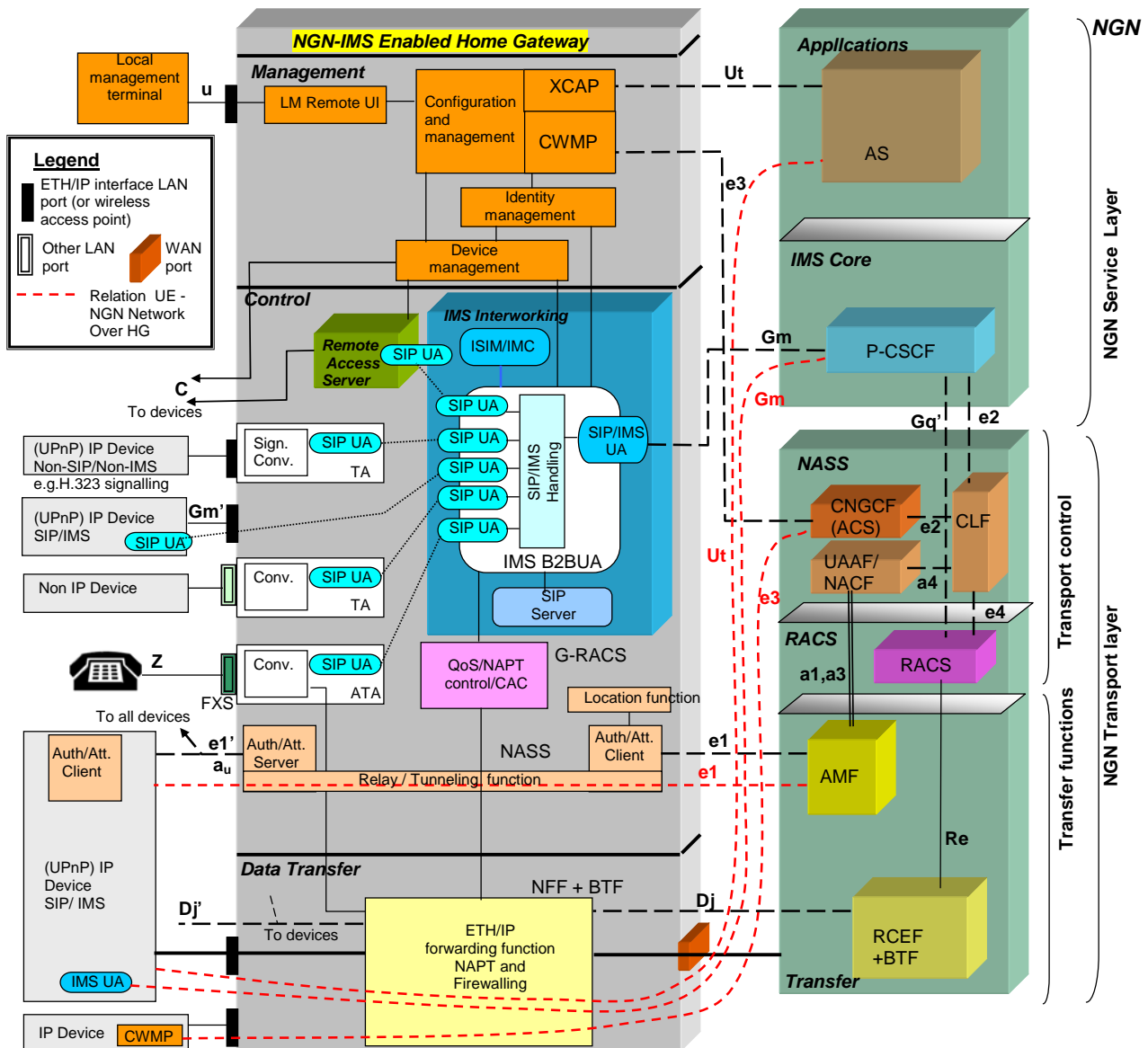


Figure 13 IMS HG functional architecture interworking with its NGN-IMS environment

6.1 IMS Interworking block

The IMS interworking block includes the IMS B2BUA, ISIM/IMC and SIP Server blocks.

The IMS B2BUA interfaces via an SIP/IMS-UA entity to the WAN side and via multiple SIP-UA entities towards the LAN side. The SIP/IMS-UA at the WAN side performs the signalling towards P-CSCF in the IMS Core. The interworking between both sides is done by a SIP/IMS handling block that is supported by an ISIM/IMC application and a SIP server. The ISIM/IMC block includes the ISIM/IMC application and can be located on a UICC card (ISIM) or in IMS HG software (IMC). The identity management blocks and device management blocks are supporting the IMS interworking block for keeping track of home devices and user identities.

The IMS Interworking block performs a number of functions, some of them are:

- Mapping of IMS signalling on the WAN side to SIP signalling on the LAN side.

- IMS Authentication and Registration of IMS HG against the IMS system, using an authentication algorithm (IMS AKA, HTTP Digest) based on the credential stored in the IMS authentication function inside the ISIM/IMC block.
- Local authentication of home SIP devices (example is use of HTTP Digest).
- Registration of home SIP devices in the SIP server (Registrar).
- Registration of Users (IMPUs) in IMS.
- Authorization of RA users based on P-Asserted identities (if RA is supported).
- Internal communication against internal SIP UAs in HG, to enable IMS services against:
 - FXS port Analogue Terminal Adapter (ATA).
 - Terminal Adaptors for legacy IP devices, or to other non-IP devices.
 - RA-block, to enable a connection between the RA-block and the authorized Remote User.

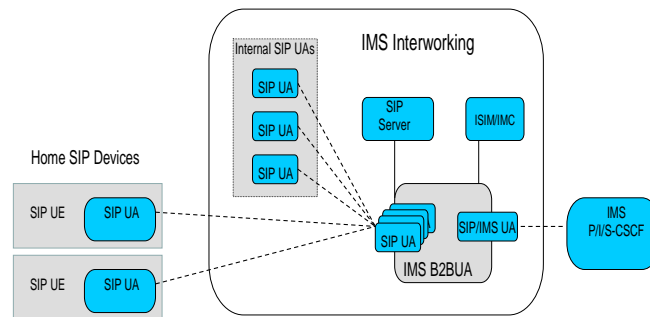


Figure 14 IMS and SIP signalling overview for the IMS B2BUA

6.1.1 The Back-to-Back User Agent (B2BUA)

A Back-to-Back User Agent (B2BUA) within the IMS interworking block is a logical signalling and call handling entity that after receiving a SIP request can reformulate it and send it out as a new request. Responses to the requests can also be reformulated and sent back in the opposite direction. A B2BUA may create the illusion of an end-to-end dialog by coupling two dialogs and forwarding messages transparently, but it always terminates dialogs between SIP-UAs.

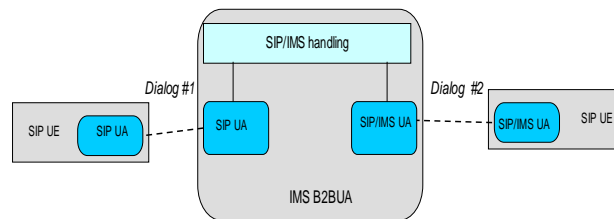


Figure 15 Generic representation of an IMS B2BUA

The main advantage of a B2BUA is its capacity to manage and monitor the entire call state and parameters. It can process even the body of a SIP message and has full control over all parameters and headers. Thus, a B2BUA is able to:

- Monitor the state and parameter of all incoming and outgoing SIP calls (e.g. a B2BUA can collect from the SDP payload the list of codecs that can be used during the call or the ports that are going to receive the media traffic).
- Interact with the CAC, the NA(P)T, or the firewall to ensure the viability of the call (e.g. from the monitored data a B2BUA can estimate the QoS requirements and check with the CAC block (G-RACS) if the IMS HG can provide the required bandwidth).
- Create or reformulate requests/responses and send it out as new requests/responses (e.g. a B2BUA can change (if necessary) IP addresses and port numbers in the incoming or

outgoing SIP messages and can also drop/generate SIP messages in order to provide the required interoperability between different SIP profiles).

- The IMS B2BUA block is able to use the information stored in an ISIM/IMC security module to authenticate the home gateway against the IMS network. The IMS signalling extends the SIP signalling, and IMS signalling procedures are according to 3GPP TS 24.229 [8] and 3GPP TS 24.503 [35] . Procedures to be supported are P-CSCF discovery, (de)registration (including authentication), session control, and more. For authentication both IMS-AKA and HTTP Digest authentication are supported using the ISIM and IMC application respectively.
- An IMS B2BUA can implement the routing behavior of a “SIP proxy”, but the IMS B2BUA does not comply to a SIP Proxy as specified in RFC3261 [7] in terms of SIP message processing.

6.1.2 The WAN side SIP/IMS UA

The WAN side entity called SIP/IMS UA is able to support:

- IETF SIP signalling (IETF SIP signalling profile), or
- The extended 3GPP IMS signalling (3GPP SIP signalling profile)

The 3GPP SIP signalling profile is an extension of the IETF signalling (both with regard to messages used and message fields), in particular providing a Secure Association (SA) between the signalling parties, and providing extended QoS capabilities. See also section 4.4 “SIP extensions for IMS” for further information.

Irrespective of the profile, the SIP/IMS UA entity communicates in the NGN network with the P-CSCF (Proxy Call State Control Function) entity, which is the first contact point for the IMS HG, on the SIP level communication. The P-CSCF serves the SIP/IMS requests directly or sends them to other network servers. Before any SIP/IMS session can be setup, the IMS HG needs to perform the following procedures:

- P-CSCF server discovery, for example by using DHCP option 120 and DNS.
- First Registration to IMS:, including authentication, authorization and association.

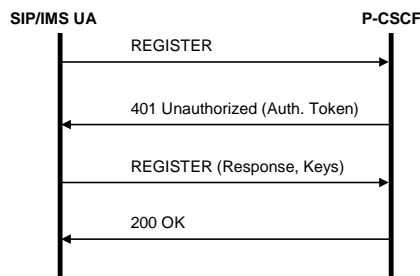


Figure 16 First Registration procedures

- Re-registrations can happen later without authentication.
- In case the IMS HG wants to be notified of certain events, a subscription must be requested for these events.

The IMS signalling communication happens between the SIP/IMS UA and the P-CSCF over the Gm reference point. The definition of this reference point is made in ETSI TS 282 007 [31].

6.1.3 SIP Server

The SIP registrar server supports local registration of home SIP IETF devices in cooperation with the device management block and the identity management block. The registration of SIP devices is also used to enable “intra LAN services” inside the HN, with use of “short” names.

A SIP Registrar is able to register SIP devices located in the home network or internally in the IMS HG itself. Those SIP devices need to be authenticated against the SIP Registrar, using one of following two cases:

- Devices not supporting authentication, or using preconfigured username/password in the IMS HG. This is typically used for devices that are not able to perform authentication (e.g. old legacy POTS phone).
- SIP devices allowing different home users to log in using own credentials. Each user of such a device needs to authenticate against the SIP Registrar (an example is the family PC). A particular home user, identified by an IMPU is then registered in the IMS network by the IMS Interworking block in the IMS HG, indicating that this user is available.

The HGI-RD001-R2 specification [1] requires (R291) that the SIP registrar distinguishes among SIP register messages coming from a non-IMS device and those register messages coming from an IMS SIP device. When such IMS and non-IMS devices are registered in the SIP registrar server, those devices are part of the home network.

6.1.4 ISIM/IMC

The ISIM/IMC block in the IMS Interworking sub-block includes the ISIM security module or the IMC security module. The ISIM/IMC security module contains the needed parameters for IMS core interaction. Examples of parameters are IMS subscription parameters like IMPI (private identity), IMPUs (public identities), Home Network IMS URIs (WAN domain) and long term secrets [29]. These parameters are provisioned on an UICC card in case of an ISIM application [30]. When using an IMC security module these parameters are provisioned in another way, one alternative is to use the TR-069 protocol. See section 4.2 for more information around ISIM/IMC security.

Note that the ISIM/IMC applications support multiple IMS public identities (IMPUs) assigned to one IMS Private Identity (IMPI).

6.2 Interworking with the HG Resource and Admission Control Subsystem (G-RACS)

The IMS Interworking block interacts with the internal home gateway Resource and Admission Control Subsystem (G-RACS). This function includes NA(P)T control, Firewall control, QoS handling, and Connection Admission Control (CAC) functions. Note that in HGI-RD001-R2 specification [1], this function is similar to the IMS RACS function in the network, but has no relation/interfaces to it. This control function is controlling the filtering and forwarding block providing the data transfer functions in the home gateway.

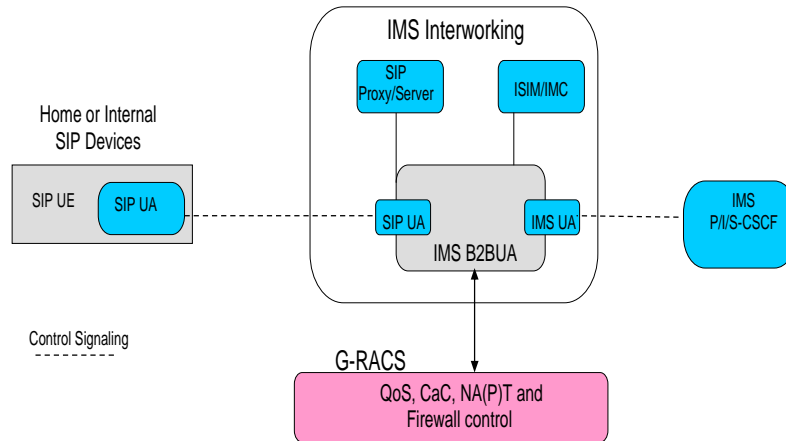


Figure 17 Interaction between IMS Interworking block and the G-RACS

6.2.1 NA(P)T and Firewall control functions

The opening of ports in the NA(P)T and Firewall for the media traffic can either be done “static” or “dynamic”.

- Static configuration of ports to be used can be configured by the ACS.
- Dynamic configuration of ports to be used can be done from the IMS B2BUA, via the NA(P)T and Firewall control function.

The NA(P)T and Firewall function in G-RACS acts as a filter, at the boundary between the LAN and the WAN networks. The IMS B2BUA can perform an effective NA(P)T and firewall traversal solution. For media streams, it can interact with the NA(P)T mechanism to provide the required bindings and with the firewall to open the required ports. During SIP control signalling resources (IP addresses/ports) can be reserved via this control block and included in the signalling messages. As soon as a confirmation arrives, an effective allocation of resources can happen.

6.2.2 QoS handling and CAC

By reading the SIP control messages, the IMS B2BUA can obtain the list of codecs that can be used in a multimedia session, estimate the bandwidth required for the most bandwidth consuming codec, and interact with the “QoS handling” and “CAC” block (G-RACS) in order to check whether there are enough bandwidth resources to support the connections, and whether the required QoS priority queues are enabled. This entity is responsible for the admission control within the home network. Typically, a new session must be refused if no bandwidth resources are available on the envisaged physical interfaces. Also limitations of the number of sessions may be performed to prevent the risk of congestion within the HN. This entity communicates with the IMS B2BUA for QoS and bandwidth. In particular the entity:

- Checks resources availability on each link/device involved in the communication requesting a QoS and bandwidth reservation/allocation, through an internal database.
- Performs the appropriate resources reservation based on an internal Policy Control Function (PCF). The HGI class based QoS approach is described in HGI-RD001-R2 specification [1] in section 7.8.12. This PCF function conforms to the PCF function defined in ETSI TS 185 003 [14]. The internal policy control is supposed to integrate a database containing the access profile. This includes bandwidth and QoS parameters for the applications and terminals, which could be configured by a user.

For instance, congestion issues within the HN may be solved defining resources for several SSIDs.

6.3 Signalling to LAN side SIP UAs

Each SIP UA instance at LAN-side of the IMS B2BUA is communicating to a peer SIP UA entity inside the IMS HG or to a peer SIP UA inside a SIP device in the home network.

The internal SIP UA blocks generate SIP messages for the home devices that do not have a SIP stack on board. The LAN side SIP UA in the IMS B2BUA communicates with these SIP UAs so that IMS services can be delivered to that home device. The SIP UAs for the TAs that are considered in [1] are related to (see Figure 13):

- IP Devices and Non IP Devices in the home network: A Terminal Adapter (TA) together with the SIP UA need to be defined, not part of HGI-RD001-R2 specification.
- FXS(s) ports: A Terminal Adapter (TA) together with the SIP UA that connects legacy POTS/ISDN phone(s). Note that FXO port not is part of HGI-RD001-R2 specification. IMS related requirements for the FXS port(s) is in R278 to R284.
- Remote Access block: A SIP UA is needed for that functional block. The Remote Access block uses the local identity mapped to IMS identity and device capabilities of the local devices, based on UPnP and DHCP, and handled by the Identity Management and Device Management function blocks. The remote access rights (on a per IMS user basis) to local devices can be configured in an Access Control List (ACL). Functionality for the remote terminal to find devices and corresponding services on the LAN is also supported (Synchronization). Remote Access as defined in the HGI-RD001-R2 specification [1] is in detail described in a HGI Guideline paper named "Remote Access" [2]. In Appendix, an introduction to IMS based Remote Access is included.

6.4 NASS related control functions in IMS Enabled HG

NASS related control functions (see Figure 13) are assuring a basic connectivity to the network, and as such, need to be performed before any SIP/IMS related functions. The connectivity considered can be categorized as:

- Connectivity of IMS enabled HG to the network.
- Connectivity of home devices to the IMS enabled HG.
- Connectivity (transparent) for home devices to the network over the IMS enabled HG.

The NASS related control functions in the network (see Figure 2 and 3) are AMF, UAAF, NACF and CLF. The AMF is a 'merging' function of the authentication procedures and IP configuration procedures for network access. The related protocols in the HGI-RD001-R2 specification [1] are PPP and DHCP server entities. For these protocols the AMF/UAAF and NACF can be considered as one protocol block all together.

When PPP is used, related UAAF is the CHAP protocol and NACF is the IPCP protocol. When DHCP is used between IMS HG and network for Residential Profile v1.0, the authentication is in some way implicit (UAAF=nihil) and NACF is the DHCP protocol.

The function in the IMS enabled HG related to this is the block called Authentication/Attachment Client at the HG WAN side. Again this is represented by the PPP or DHCP protocol, but now on the client side entity. During the exchange of configuration parameters, there can also be an exchange of location information between the HG and the CLF function in the NASS. Note that according to TS 185 003 [14], the location information may also be available via another way, e.g. configured by the home administrator. The function in Figure 13 dealing with the location information in the home gateway named Location function.

At the LAN side only DHCP is used for home devices in order to get a private IP address configuration from the home gateway, in case of NA(P)T. This may be preceded by an authentication function, like Wi-Fi WPA authentication for Wi-Fi devices. The server function in the home gateway is a combination of WPA and DHCP, both server side protocol entities, in general called Authentication/Attachment Server block.

Some home devices may want a public IP address configuration, e.g. IMS enabled devices. In that case the DHCP communication is relayed in the HG between the device and network. If there is any network access authentication procedure, then the authentication messages must be tunnelled between the devices and the network. The relaying and tunnelling is performed in the HG in the block called Relay/tunnelling.

6.5 Configuration and management

The configuration and management block in Figure 13 is the concatenation of home gateway and home devices management and application service management. The respective NGN reference points and protocols are:

- e3 reference point and CWMP protocol (TR-069 or beyond) for HG management.
- Ut reference point and XCAP protocol for application service management.

The configuration and management block also interacts with the Identity- and Device-management blocks. In Residential Profile v.1.0 specification the Management architecture is described in section 7.7 and the general Management requirements are in section 8.6. Specific IMS HG related configuration and management requirements are also included in the specific IMS requirement sections.

6.5.1 CWMP (TR-069) based management

The reference point e3 is defined in ES 282 004 [13] and TS 183 003 [14]. It represents the interface between a CWMP client (user side) and a CWMP server network side, where the TR-069 protocol and updates is indicated as the default protocol for home gateway management, and TR-098 and updates is the related data model for the IMS HG. The IMS HG functional architecture (see Figure 13) also defines (in line with TR-069) transparent home device management over the e3 reference point. The ETSI documents also state that the CNGCF represents the ACS entity.

When the IMS HG supports interworking with IMS and Remote access functions in general, it is clear that a number of new IMS objects and parameters could be added to the TR-069 data models (TR-098, TR-104 etc.) as extensions, but it is not in the scope of this document to list such extensions.

6.5.2 XCAP based management

The reference point Ut is defined in HGI-RD001-R2 specification [1] as the interface between the IMS HG and the Application Server(s) in IMS. The Ut interface is also defined by ETSI TISPAN in TS 185 006 for home devices [15]. A number of Application Server protocols may be used on the related interface.

The HGI-RD001-R2 specification [1] indicates the XML Configuration Access Protocol (XCAP) to be used (R277 and R278 in [1]). XCAP allows a client to read, write and modify application configuration data, stored in XML format on a server. XCAP is not a new protocol. XCAP maps XML document sub-trees and element attributes to HTTP URIs, so that these components can be directly accessed by HTTP.

6.5.3 Identity management block

The Identity management block manages the local identities (used at the LAN side), the IMS public identities IMPUs (used at the WAN side) and the mapping between local and IMS identities.

- Registration of local identities to home devices is done by the end user or by the home administrator (the BSP doesn't care about local registration) in the HG.
- Registration of local credentials for home users (contact address and Username /Password). Usually not all users located in the CPN should have access to the functionalities of the IMS B2BUA. To support that feature, SIP Digest authentication may be requested to SIP UAs located in the CPN (or in the HG) at the registration phase. Therefore, there is a need to store some local credentials that must be used to authenticate home users and to register any local address-of-record (AOR). An AOR is a SIP URI that points to a domain with a location service that can map the URI to another URI where the user might be available. Typically, the location service is populated through registrations. An AOR is frequently thought of as the "public address" of the user.
- Mapping between local user identities and corresponding IMS identities (IMPUs) to be used by the IMS Interworking block.

The specific implementation of the local registration mechanism for home user was left open in the HGI-RD001-R2 requirements. The local registration and local services support requirements are in that document's section 8.8.4.4, i.e. R.288 to R.306 in [1].

6.5.4 Device management block

The Device management block stores information about home devices on the HG. This function can be implemented in the IMS HG using protocols like DHCP, SIP or UPnP at the C reference point (to locally register devices and share capabilities).

- It stores the devices capabilities on the IMS HG. The IMS HG, when it receives an INVITE, can check if there is a device in the home network, able to support that session.
- It includes information whether the device is active or not, and via which physical LAN port it is connected (device location information).
- The IMS B2BUA also needs to know the location of the home users to correctly route the sessions. That user information, which is obtained from local registration messages, consists of bindings of device location information and local AORs.

6.5.5 LM Remote UI block

The **LM Remote UI** (Local Management User Interface): Typically, but not limited to a Web-based interface. A home user can manage IMS HG parameters in the gateway from a device on the HN. HGI-RD001-R2 specification has LM Remote UI requirements in section 8.6.6 (R198-R213)

7 Home device interworking with IMS HG

Home devices interwork with the IMS Interworking block in the IMS HG directly or via a Terminal Adapter. Note that any terminal adapter can either be included in the IMS HG or located in a separate physical entity. The terminal adapter can adapt the signalling system used, the media coding, or both.

IP devices (IMS/SIP enabled or not) can be UPnP enabled or not (that is why 'UPnP' is between brackets in the IMS enabled HG block diagram). If devices are UPnP enabled, the IMS HG must discover them using the UPnP protocol. Non-UPnP-enabled devices can be discovered in other ways. The device discovery information is stored by the device management function in the IMS HG.

SIP and IMS enabled devices, during a registration process to the IMS HG, reveal the identity of the user. The information is stored by the identity management function.

IMS devices having an ISIM (and requires use of IMS AKA), directly register to the IMS Core, and authenticate themselves against the P-CSCF using the secure information on the ISIM.

Note that for any (IMS or not) device, before SIP/IMS authentication/registration/signalling can be used, there needs to be an attachment by IMS HG to the network, and by the device to the IMS HG. During this attachment procedure, also an authentication may be needed in order to get network access. So be aware that a device, also an IMS device, may need to authenticate twice: first on the lower layers, for network access, and later on the application layer, for service access.

7.1 Non-IP devices

Non-IP devices don't support IP based signalling nor IP based data. A Terminal Adapter (TA) is needed requiring conversion for both signalling and data.

The signalling converter is converting the legacy signalling into SIP, and as such the converter is acting as a SIP UA towards the IMS interworking block.

The data is coded/transposed into an SIP supported format, and transferred to the network via the forwarding function.

7.1.1 Special case: Analogue Terminal Adapter = ATA

In case the non-IP device is a POTS set, and connected to the IMS HG via a FXS port, the TA is an Analogue Terminal Adapter (ATA). The POTS analogue signalling is translated into SIP/SDP and the voice is encoded into PCM or using another voice coding standard.

HGI-RD001-R2 specification [1] also specifies a number of requirements for telephony based interfaces, e.g. supported codecs and fax service support.

7.1.2 Other adapters supported by HGI-RD001-R2

The following non-IP interfaces are also supported by the HGI-RD001-R2:

- ISDN basic access.
- DECT.
- DECT NG.

7.2 IP devices (non-SIP, non-IMS)

IP devices support some form of media coding which can be encapsulated in IP packets, but may use a form of IP based signalling which is not SIP, e.g. H.323.

The media coding can be kept, but the signalling needs to be converted to SIP, so the TA in the IMS HG basically contains a signalling converter.

7.3 IP devices (SIP enabled)

This type of home device has a SIP UA (IETF profile) included. No Terminal Adapter is needed in the IMS HG. For signalling the SIP enabled home device interfaces to a SIP UA in the IMS Interworking block.

7.4 IP devices (IMS/SIP enabled)

This type of home device has an IMS UA (3GPP SIP profile) included. For IMS/SIP signalling the device interfaces directly to the NGN network (through the firewall), not using the IMS Interworking block in the IMS HG.

8 References

- [1] HGI-RD001-R2; http://www.homegatewayinitiative.org/publis/HGI_V1_Residential.pdf
- [2] HGI Guideline paper: Remote Access;
http://www.homegatewayinitiative.org/publis/HGI_remote_access_v1.01.pdf
- [3] IST MUSE II Project Deliverable DTF3.4, "Specification of a multi-service RGW with multi-provider functionality" https://www.ist-muse.org/Abstracts/abstract_DTF3.4.htm
- [4] IST MUSE II Project Deliverable DTF3.3 - Part 2, "Specification of an advanced, flexible, multiservice Residential Gateway - Part 2: http://www.ist-muse.org/Abstracts/abstract_DTF3.3.htm
- [5] SIP and IMS Residential Gateway, Broadband Europe 2007 conference paper (Tu4A-2) [http://www.bbeurope.org/BBE2006,paper we4a1](http://www.bbeurope.org/BBE2006,paper%20we4a1)
- [6] T. Cagenius et al, "An IMS Gateway for Service Convergence in Connected Homes", 45th Congress of the FITCE, Athens (Greece), August 2006
- [7] IETF RFC 3261, "SIP: Session Initiation Protocol", June 2002
- [8] 3GPP TS 24.229 V8.6.0, "IP Multimedia call control protocol based on SIP and SDP", December 2008
- [9] 3GPP TS 24.930 V7.1.0, "Signalling flows for the session setup in the IM CN Subsystem based on SIP and SDP", March 2007
- [10] 3GPP TS 33.203 V7.5.0, "Access security for IP based services", March 2007
- [11] Virtually at home: High-performance access to personal media, Ericsson Review 2008-Q2 http://www.ericsson.com/ericsson/corpinfo/publications/review/2008_02/files/2_RemoteAccess.pdf
- [12] ETSI ES 282 001 v2.0.0, "NGN functional architecture"
- [13] ETSI ES 282 004 v2.0.0, "Network Attachment Sub-System (NASS)"
- [14] ETSI TS 185 003 V2.0.0 "CNG Architecture and Reference Points"
- [15] ETSI TS 185 006 V2.0.0 "Customer Devices Architecture and Reference Points"
- [16] ETSI TR 185 007 V2.0.0 March 2008 "Analysis of protocols for customer networks connected to TISPAN NGN"
- [17] 3GPP TS 23.228 v8.2.0, "IMS Stage 2", September 2008
- [18] 3GPP TS 22.173 v8.3.0, "IMS Multimedia Telephony Service and supplementary services; Stage 1", June 2008
- [19] 3GPP TR 22.940 v7.0.0, "IMS messaging", December 2007
- [20] 3GPP TS 22.141 v.7.0.0, "Presence Service; Stage 1", Dec. 2007
- [21] 3GPP TS 24.247 V8.1.0, "Messaging service using the IP Multimedia Core Network subsystem; Stage 3", March 2008
- [22] 3GPP TS 24.141 v8.1.0, "Presence service using the IP Multimedia Core network subsystem; Stage 3"
- [23] OMA-TS-SIMPLE_IM-V1_0-20070816-C, "Instant messaging using SIMPLE", Aug 2007
- [24] OMA-TS-Presence_SIMPLE-V1_1-20080128-C, "Presence SIMPLE specification", Jan 2008
- [25] Open IPTV Forum-Functional Architecture – v1.1, Jan 2008:
http://www.openiptvforum.org/docs/OpenIPTV-Functional_Architecture-V1_1-2008-01-15_APPROVED.pdf

-
- [26] 3GPP TS 22.800 v.6.0.0, “IMS subscription and access scenarios”
 - [27] IETF RFC 2396, Uniform Resource Identifiers (URI), August 1998
 - [28] IETF RFC 2806, URLs for Telephone Calls, April 2000
 - [29] 3GPP TS 31.103, “Characteristics of ISIM application”
 - [30] 3GPP TS 31.101, “UICC terminal interface”
 - [31] ETSI ES 282 007, IP Multimedia Subsystem (IMS); Functional architecture
 - [32] ETSI ES 282 003, RACS Functional Architecture
 - [33] 3GPP TR 21.905 Vocabulary for 3GPP Specification
 - [34] ETSI TS 185 010, Customer Premises Protocol Specification, Stage 3 Specification (draft)
 - [35] 3GPP TS 24.503, 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]
 - [36] ETSI TS 187 003, Security Architecture NGN-R1

9 Acronyms

3GPP	3 rd Generation Partnership Project
A-xxx	A ccess Network Function. Ex. A-RACS
ACL	Access Control List
ACS	Auto-Configuration Server
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Layer Gateway
AKA	Authentication and Key Agreement
AMF	Access Management Function
AN	Access Network
AOR	Address Of Record
AP	Access Point
ARF	Access Relay Function
AS	Application Server
ASF	Application Server Function
ATA	Analogue Terminal Adapter
AtF	Attachment Function
ATM	Asynchronous Transfer Mode
AuF	Authentication Function
B2BUA	Back to Back User Agent
BGF	Border Gateway Function
BRAS	Broadband Remote Access Server
BSP	Broadband Service Provider
BTF	Basic Transport Function
C-xxx	C ore Network Function. Ex. C-BTF
CAC	Call Admission Control/Connection Admission Control
CBR	Constant Bit Rate
CE	Consumer Electronics
CHAP	Challenge-Handshake Authentication Protocol
CLF	Connectivity session Location and repository Function
CND	Customer Network Device (=Home Device (HN))
CNG	Customer Network Gateway (=Home Gateway (HG))
CNGCF	Customer Network Gateway Configuration Function
CoS	Class of Service
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CSCF	Call Session Control Function

CSMF	Communication Services Media Function
CWMP	CPE WAN Management Protocol
D-xxx	CND (=HD) D evice function, ex. D-RACS
DA	Destination Address
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DS	Downstream
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
EAP	Extensible Authentication Protocol
ECF	Elementary Control Function
ED	End Device
EFF	Elementary Forwarding Function
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute
EU	End User
FMC	Fixed Mobile Convergence
FXO	Foreign eXchange Office
FXS	Foreign eXchange Subscriber
G-xxx	CNG (=HG) Home G ateway function
GUI	Graphical User Interface
HG	Home Gateway (=RGW=CNG)
HGI	Home Gateway Initiative
HLR	Home Location Register
HN	Home Network
HSS	Home Subscriber Server
HTTP	HyperText Transfer Protocol
I-BGF	Interconnection-Border Gateway Function
I-CSCF	Interrogating-Call Session Control Function
IBCF	Interconnection Border Control Function
ISC	Reference Point between a CSCF and an Application Server.
ICSI	IMS Communication Service Identifier
IGMP	Internet Group Management Protocol
IETF	Internet Engineering Task Force
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity
IMS	IP Multimedia Subsystem
IP	Internet Protocol

IPCP	PPP Internet Protocol Control Protocol
IPsec	IP Security
IPTVF	IPTV Function
IPv4	Internet Protocol version 4
ISIM	IP Multimedia Services Identity Module
ISP	Internet Service Provider
L2TP	Layer 2 Tunnelling Protocol
LAN	Local Area Network
LF	Location Function
LM Remote UI	Local Management Remote User Interface
MAC	Media Access Control
NACF	Network Access Configuration Function
NAPT	Network Address and Port Translation
NA(P)T	Network Address and (Port) Translation
NASS	Network Attachment SubSystem
NAT	Network Address Translation
NFF	NAPT and Firewall Function
NGN	Next Generation Network
NTF	NAPT Transversal Function
OAM	Operations, Administration & Maintenance
OSA	Open Service Access
OSI	Open Systems Interconnection
P-CSCF	Proxy-Call Session Control Function
PBX	Private Branch Exchange
PDBF	Profile Data Base Function
PES	PSTN/ISDN Emulation Subsystem
PIN	Personal Identification Number
POTS	Plain Old Telephone Service
PPF	Plug and Play Function
PPP	Point-to-Point Protocol
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Connection
QoS	Quality of Service
RA	Remote Access
RACF	Resource and Administration Control Function
RACS	Resource and Admission Control Subsystem
RADIUS	Remote Access Dial In User Service
RCEF	Resource Control Enforcement Function

RFC	Request For Comments
RGW	Residential Gateway (=CNG=HG)
S-CSCF	Serving CSCF
SA	Source Address
SIP	Session Initiation Protocol
SLF	Subscription Locator Function
SP	Service Provider
SPDF	Service based Policy Decision Function
SSID	Service Set Identifier
STB	Set Top Box
TA	Terminal Adapter
TE	Terminal Equipment
TISPAN	Telecoms & Internet converged Services & Protocols for Advanced Networks
UA	User Agent
UAAF	User Access Authorisation Function
UE	User Equipment
UI	User Interface
UPnP	Universal Plug&Play
UPSF	User Profile Server Function
URI	Uniform Resource Identifier
Ut	Reference Point between UE (and IMS HG) and an Application Server
VLAN	Virtual Local Area Network
VoD	Video on Demand
VoIP	Voice over IP
WAN	Wide Area Network
XCAP	XML Configuration Access Protocol

10 Definitions

The definitions and terms used in this IMS Enabled HG guideline document make use of the definitions defined in HGI-RD001-R2 document.

10.1 Definitions from HGI-RD001-R2

In HGI-RD001-R2 [1], the definitions can be found in chapter 3, below is a subset of those definitions:

- **LM Remote UI** (Local Management User Interface): UI (typically, but not limited to, a Web-based) to let a user manage the RM client on the gateway from a device in the HN.
- **Managed Device**: device that has a remote management client that communicates directly or indirectly (via the HG) with a remote management server.
- **Managed service**: A service for which the BSP provides preferential treatment (that can include QoS) for the customer. The service can be a service offered by the BSP or operated by the BSP on behalf of a third party. A managed service can also be local: watching a video on a PC recorded on the IPTV STB; as explained in the IPTV PVR use case. Managed services do not necessarily involve use of the remote management system; management only means that the operator has taken some responsibility for the service (e.g. its QoS treatment) in order to provide the appropriate quality of experience.
- **Remote Management System (RMS)**: the management entity which includes the Auto-Configuration Server capabilities but also provides additional management functionalities. The RMS includes resource and device inventory, event notification and alarm management, diagnostics and troubleshooting.
- **Use case**: Description of a general user need. It contains the context of usage behaviour that meets the need and serves as an umbrella scenario. Example is Voice communication.

10.2 Other Definitions used in this document

In HGI-RD001-R2 section 7.5.2 a big number of “definitions” are also defined, those are included below. In addition definitions for CND, CNG, IMS Terminal, Terminal Adapter, IMS Credentials (IMC), IMS application and Pre-IMS AKA have been added:

- **B2BUA**: an IMS B2BUA terminates one SIP session (generated by a SIP non-IMS UA) and translates it into an IMS session to the IMS core and vice versa. It maps IMPUs to local identities through the Identity Management module. It involves an authentication algorithm (IMS AKA, HTTP Digest).
- **Customer Network Device (CND)**: home network device enabling the final user to have direct access to services through a specific user interface. (TISPAN definition, in HGI called HD)
- **Customer Network Gateway (CNG)**: home network device acting as a gateway between the home network and the NGN and able to perform networking functions from physical connection to bridging and routing capabilities (L1-L3), but also possibly implementing functions related to the service support (up to L7). (TISPAN definition, in this document called IMS enabled HG or just IMS HG)
- **Device management**: stores device capabilities on the HG. This function can be implemented using protocols like SIP or UPnP (to locally register devices and share capabilities).
- **Home Gateway**: device connecting the HN to the Internet and Service Platforms.

- **Identity management:** maps the IMS identity stored in the HG to a local identity. Devices should first register locally with the HG and then the HG registers to the IMS core.
- **IMS Credentials (IMC):** A set of IMS security data and functions for IMS access by an IMS terminal not having an ISIM or USIM module. The IMC is not including an ISIM or a USIM. The IMC is not used if ISIM or USIM is present.
- **IMS Interworking:** mapping external IMS messages to internal (home) devices and vice versa. The main blocks are SIP UAs, IMS B2BUA, SIP server and ISIM/IMC.
- **IMS terminal (UE):** is preconfigured with a proxy CSCF URL, discovers that proxy with DHCP. The IMS UE is a general concept indicating a home environment in which an entity including a SIP IMS UA is implemented. In general, the UE can be the CNG and the CND or just the CND (in this case there is no CNG in the home network). (TISPAN definition)
- **ISIM application:** The ISIM application contains the needed parameters for IMS core interaction, when IMS AKA is used as authentication method. See also ISIM module definition.
- **ISIM module:** stores IMPIs (private identities), IMPUs (public identities), Home Network IMS URIs (WAN domain) and long term secrets, and takes part in ISIM based authentication (IMS AKA)¹.
- **Location Function:** provides applications with location information configured by the BSP (received from the CNGCF or obtained from the network), typically through DHCP.
- **Pre-IMS AKA:** TISPAN has defined the possibilities for SIP devices in the home to make use of the so called NASS-IMS Bundled authentication or HTTP Digest for authentication against IMS Core.
- **Remote Access:** uses the local identity mapped to IMS identity and device capabilities of the local devices, based on UPnP and DHCP, handled by the Identity Management and Device Management function blocks. The remote access rights (on a per IMS user basis) to local devices can be configured in an ACL. Functionality for the remote terminal to find devices and corresponding services on the LAN is also supported (Synchronization).
- **Security:** covers local access authentication, network authentication of the HG and firewalling.
- **Self provisioning:** enables the user to modify some service configurations through a (Web) User Interface (UI) on LAN side, at the Application Server (IMS) (and/or locally). Note that self-provisioning is not the initial provisioning (which is made by the ACS through the e3 interface).
- **SIP proxy/server:** supports local registration of SIP devices (including the SIP registrar function) and proxy functionalities in cooperation with the Identity Management block.
- **SIP UA:** generates SIP messages for devices that do not have a SIP stack on board (IP devices, legacy/POTS devices ...). The SIP UA logic may be different for each type of device.
- **Terminal Adapter (TA):** a B2BUA only understands the SIP protocol. To extend the exposed functionalities to those terminals which do not support SIP, some terminal adapters (TAs) will be required. Those TAs can be implemented in the RGW or deployed in the CPN (e.g. at a FXS ports to connect a legacy phone to the RGW or at a FXO port to connect the RGW to the PSTN) and must include a signalling converter (Sign. Conv.) to act as SIP UAs and to facilitate a total interoperability with the B2BUA. In addition a terminal adapter converts the analogue voice to a digital signal using a codec.

¹ Note that the ISIM is optional (in the case of adoption of HTTP Digest), in this case identities and keys for authentication must be handled in another way.

11 Important notice, IPR statement, disclaimer and copyright

The Home Gateway Initiative (HGI), formed in 2004, is an industry forum of Service Providers and Home Gateway, chip, software and other vendors, driving the architecture for the Home Network. HGI sets the technical requirements for Home Gateways and Home Networks that meet the service and business needs of Service Providers. The intention is to increase the cost-effectiveness of Home Gateways and Home Networks by taking a global approach, involving the worldwide vendor and Service Provider community, referring to existing standards wherever possible, and working alongside other standard development organizations wherever gaps and inconsistencies in or between existing standards are identified. More about HGI can be found at www.homegateway.org.

This document is the output of the Working Groups of the HGI and its members as of the date of release. Readers of this document must be aware that it can be revised, edited or have its status changed according to the HGI working procedures.

The HGI makes no representation or warranty on the contents, completeness and accuracy of this publication.

This document, though formally approved by the HGI member companies, is not binding in any part on the HGI members.

IPRs essential or potentially essential to the present document may have been declared in conformance to the HGI IPR Policy and Statutes available at the HGI website www.homegateway.org.

Any parts of this document may be freely reproduced (for example in RFPs and ITTs) by HGI and non-HGI members subject only to the following:

- HGI Requirement numbers not being changed
- an acknowledgement to the HGI being given in the resulting document.

Trademarks and copyrights mentioned in this document are the property of their respective owners.

The HGI membership list as of the date of the formal review of this document is: 2 Wire, Inc., Alcatel-Lucent, Arcor, AVM, Belgacom, BeWAN, Broadcom, BT, Cisco, Comtrend, Deutsche Telekom, D-Link Corporation, DS2, DSP Group, Echelon EMEA, Entropic Communications,, Ericsson AB, Fastweb SpA, France Telecom, Freescale Semiconductor, Gigaset, Gige Semiconductor, Huawei, Ikanos, Infineon Technologies AG, Intel, Intellon, JDSU, Jungo Software Technologies, KDDI, LG-Nortel Co Ltd, Marvell Semiconductors, Microsoft, Mitsubishi, NEC Corporation, Netgear, NTT, Philips, Pirelli Broadband Solutions, Portugal Telecom Sagem, Sercomm, SoftAtHome, SiConnect, Spidcom, Swisscom AG, Telecom Italia, Telefonica, Telekom Slovenije, Telekom Malaysia, Telekomunikacja Polska, Telenor, TeliaSonera, Telstra, . Thomson, Tilgin AB, TNO, U4EA Technologies Limited, Vtech, Zarlink, ZTE, ZyXEL.

12 Appendix

12.1 IMS based Remote Access

Remote Access to the home network can be implemented with or without IMS mechanisms. This section outlines an implementation example for the IMS based Remote Access as described in the HGI Guideline paper named “Remote Access” [2].

The following figure shows a high level architecture of the IMS role in enabling Remote Access to home devices from a Remote Device. The devices types of interest in the residential network for IMS based remote access are UPnP devices as well as IP devices. Remote access to SIP devices in the home is covered by the existing B2BUA functionality in the IMS enabled HG.

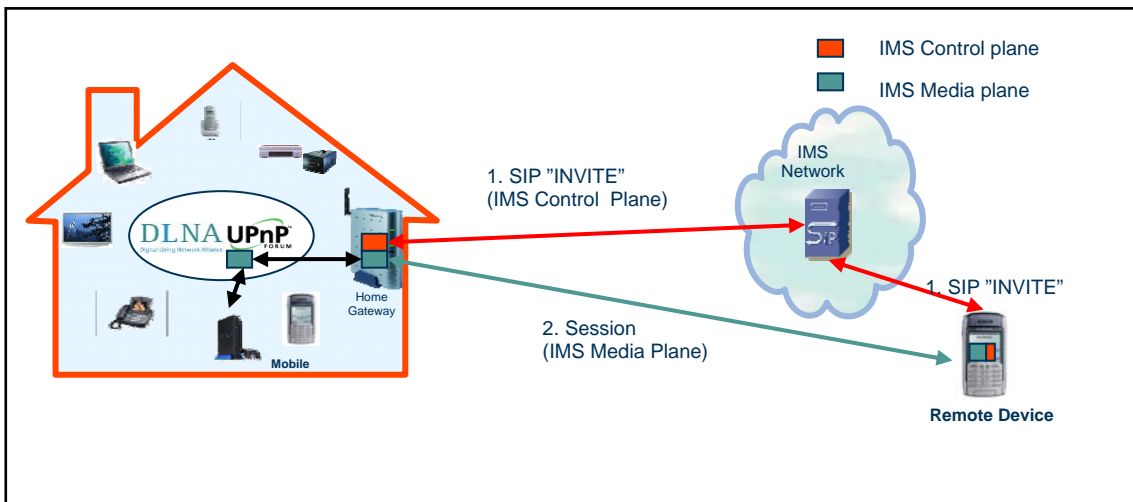


Figure 18 High level IMS based Remote Architecture: overview

The principle of “IMS based Remote Access” is that the IMS control plane is used to route the INVITE message to the HG and to set up a secure session on the IMS media plane between the Remote Device and the HG. This is the same approach as described by TISPAN in TS 185 003 [14] and in TS 185 010 [34].

The proposed architecture uses an IMS-NGN infrastructure to deliver managed remote access services end-to-end with different requirements on QoS, e.g. real-time IPTV streaming (place shifting) versus background upload of JPEG pictures. This means that IMS/SIP/SDP session control signalling will be applied for each session in the IMS Media Plane and corresponding QoS measures (transmission resource allocation and CAC) can be applied both in the Radio Access Network and Broadband Access Network.

VPN is not a pre-requisite for the IMS based remote access service, which will make it possible to increase the number of terminals to use with the service such as 2G/3G phones. The integrity and confidentiality level is the same as for basic IMS voice. As an option it shall be possible to use IPsec for IMS control plane signalling towards the P-CSCF and in the media plane towards the remote device according to TISPAN / 3GPP standards.