



Home Gateway Initiative

HGI guideline paper

Remote Access

Version 1.01

18/05/08

PAGE LEFT INTENTIONALLY BLANK

Table of Contents

Table of Contents	3
1 Important notice, IPR statement, disclaimer and copyright.....	4
2 Acronyms	5
3 Definitions	7
4 Introduction and scope of the Home Gateway Initiative (HGI)	9
4.1 Cooperation with other bodies and initiatives	9
5 Introduction	10
5.1 Scope and purpose of this document	10
6 Remote Access in HGI Residential Profile v1.0.1	11
6.1 Use Cases.....	11
6.1.1 Remote Access to home devices and content	11
6.1.2 Home Management & Security	11
7 IMS Approach for Remote Access	12
7.1 Overview	12
7.2 Architecture for IMS based Remote Access	12
7.3 IMS Enablers for Remote Access	14
7.4 Remote Access Functionality in the HG	14
7.5 Remote Access block in HGI IMS Interworking Architecture.....	15
8 Web Based Approach for Remote Access	16
8.1 Overview	16
9 Operator Controlled Remote Access	18
10 References	19

1 Important notice, IPR statement, disclaimer and copyright

The Home Gateway Initiative (HGI) is a non-profit making organization created to define guidelines and specifications for broadband Home Gateways.

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, Atheros, AVM, Belgacom, BeWAN, Broadcom, BT, Deutsche Telekom, DS2, DSP Group, Echelon EMEA, Ericsson AB, Fastweb SpA, France Telecom, Freescale Semiconductor, Gigle Semiconductor, Huawei, InAccess Networks, Infineon Technologies AG, Intel, Intellon, ITRI, JDSU, Jungo Software Technologies, KDDI, KPN, LG-Nortel Co Ltd, Linksys/Cisco, Marvell Semiconductors, Microsoft, Motorola, Netgear, NTT, Philips, Pirelli Broadband Solutions, Portugal Telecom, Sagem, Siemens, Sphairon Access Systems, Spidcom, Supportsoft, Swisscom AG, Telecom Italia, Telefonica, Telekom Slovenije, Telekomunikacja Polska, Telenor, TeliaSonera, Telkom ZA, Telstra, Texas Instruments, Thomson, Tilgin AB, TNO ICT, U4EA Technologies Limited, Ubicom Inc., Vtech, ZTE, Zarlink, ZyXEL.

2 Acronyms

ACL	Access Control List
ACS	Auto-Configuration Server
ALG	Application Layer Gateway
AN	Access Network
B2BUA	Back to Back User Agent
BRAS	Broadband Remote Access Server
BSP	Broadband Service Provider
CAC	Call Admission Control/Connection Admission Control
CE	Consumer Electronics
CNGCF	Customer Network Gateway Configuration Function
CPE	Customer Premises Equipment
CWMP	CPE WAN Management Protocol
DA	Destination Address
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DS	Downstream
DSCP	Differentiated Services Code Point
EAP	Extensible Authentication Protocol
ED	End Device
EU	End User
HG	Home Gateway
HN	Home Network
HTTP	HyperText Transfer Protocol
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPv4	Internet Protocol version 4
ISIM	IP Multimedia Services Identity Module
ISP	Internet Service Provider
LAN	Local Area Network
LF	Location Function
LM Remote UI	Local Management Remote User Interface
MAC	Media Access Control
NAPT	Network Address and Port Translation
NAT	Network Address Translation

NGN	Next Generation Network
P-CSCF	Proxy-Call Session Control Function
PIN	Personal Identification Number
QoS	Quality of Service
Remote UE	Remote User Equipment
SA	Source Address
SIP	Session Initiation Protocol
SP	Service Provider
UI	User Interface
UPnP	Universal Plug&Play
VLAN	Virtual Local Area Network
VoD	Video on Demand
WAN	Wide Area Network

3 Definitions

- **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).
- **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 IMS core.
- **IMS Interworking,** mapping external IMS messages to internal (home) non-IMS devices and vice versa. It is based on:
 - **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.
 - **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).
 - **SIP proxy/server:** supports local registration of SIP devices (it includes the SIP registrar function) and proxy functionalities in cooperation with the identity management block.
- **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.
- **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 on the HN.
- **Location Function:** provides applications with location information configured by the BSP (received from the CNGCF or obtained from the network), typically through DHCP.
- **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 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).
- **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.
- **Security:** covers local access authentication, network authentication of the HG and firewalling.

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.

- **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).

4 Introduction and scope of the Home Gateway Initiative (HGI)

Home connectivity has evolved dramatically over recent times. From the initial simple voice service, home services evolved in the 80s to include things such as fax and video text, with the 90s seeing the advent of mass-market Internet access via dial-up modems. At the start of the 21st century, the world has entered the broadband era. Network operators have deployed technology that offers much larger bandwidths, such as DSL, cable or fibre-based access systems.

The Internet has been a major driver for the evolution to broadband, creating a new experience for the customer and offering him new services such as email and Internet browsing, and “online” versions of existing services such as digital photo labs, ticket booking etc.

The next generation of broadband services (triple or even “multiple-play”) has created a set of new requirements for the Home Gateway, namely:

- the need to manage the Home Gateway, and to a lesser extent, the home network and the devices beyond the Home Gateway
- allowing the right device or application to connect to the right service platform with the right service class / Quality of Service
- unifying device capabilities in order to offer customers a better “integrated home environment”.

Due to the lack of suitable off-the-shelf and standardized products to support this new, end-to-end network and service model, several major Telecom Operators have recently worked separately with a very small number of Home Gateway vendors to specify and develop suitable Gateways. However, such custom development is not cost-effective for either operators or vendors.

It became apparent that many operators had similar service aspirations, and so were asking for similar equipment. Therefore in December 2004, nine Telecom Operators founded the Home Gateway Initiative to agree on a common Gateway specification. The intention was to involve the relevant vendor community (i.e. vendors of gateways, chipsets, software, devices and transmission systems) so that the specifications would also be pragmatic and could be realized in a cost-effective manner.

The aim of HGI is therefore to specify a small range of low cost, high capability Gateways which will provide multi-service communication support for the residential and SOHO environments. While an end-to-end network view has been taken, the specifications mainly focus on the Home Gateway device which sits between the access network and service platforms on one side, and the in-home networked devices and applications on the other.

4.1 Cooperation with other bodies and initiatives

The Home Gateway Initiative does not wish to become a new, long-term de facto standardization body. Its task is to agree a set of functional requirements for a Home Gateway, wherever possible re-using or referring out to existing specifications. An important aspect of the work is to identify gaps and inconsistencies in or between existing specifications. The HGI will publish its own specifications, but will work alongside other SDOs to ensure that issues are addressed in the most appropriate body, that there is no unnecessary duplication of effort, and that the HGI specifications are downstreamed in the most appropriate way.

5 Introduction

5.1 Scope and purpose of this document

The HGI has recognized the need to have a number of “Guideline” documents that give additional background to the requirements specified by HGI Residential Profile v1.0.1 requirements document [1]. These Guideline documents are not normative (does not add any new requirement) and are meant to help the service providers to better understand the requirements when designing an HGI inspired Home Gateway.

This Guideline document on “Remote Access” provides background information with respect to the Remote Access requirement specified in HGI Residential Profile v1 requirements document [1].

In the HGI Residential Profile v1 document [1], the HGI reference architecture defines the Remote access functionality in two sections: Remote Device Access (section 7.1.13) and IMS-based remote access (section 7.2.1) respectively.

The Remote Access requirement belongs mainly to the following sections in [1]:

- Remote End-Device Access (section 8.7)
- Authentication and Authorization (section 8.7.1)
- Remote Access Configuration (section 8.7.2)

Two different types of Remote Access have been specified in HGI Residential Profile v1 [1], Web Based Approach and IMS based Approach. When it comes to Authentication and Authorization requirements, these requirements have been separated:

- Web Based approach (section 8.7.1.1)
- IMS approach (section 8.7.1.2)

Beside the Web Based approach and the IMS based approach the HGI specification [1] gives the possibilities for the RMS system to enable Remote End-Device Access from a Remote device. Example can here be a managed security service, to a web-camera in the home. The requirement(s) can be found in the Remote End-Device Access section (section 8.7 in [1]). This alternative method, “Operator Controlled Remote Access” is described in chapter 9.

6 Remote Access in HGI Residential Profile v1.0.1

6.1 Use Cases

Remote access to home devices and content is one of the latest consumer market trends. There are several areas of use cases developed for Remote Access where the Home Gateway is required to protect access to the home network resources. Below follow a summary of the relevant Remote Access use cases from HGI Residential Profile v1.0.1 document [1]. The use cases have been divided into two groups:

6.1.1 Remote Access to home devices and content

Two use cases have been developed for content related Remote Access [1]:

- Remote access for recording video content. Mr Martin accesses his Personal Video Recorder (PVR) to initiate a recording remotely.
- Accessing content stored in the home: Mr Martin can upload/download photos or videos from local storage (e.g. PVR, networked hard disk) from a remote location.

6.1.2 Home Management & Security

Users want to be able to manage their digital home and be in control of their environment from remote. Example of use cases are here [1]:

- Home Surveillance: Mrs. Martin being able to check, via a web camera, that her children have returned home while she is still in her office.
- Home Security: The home security usage scenario is about Mr Martin using an intrusion detection and alarm system provided over broadband.
- Home Automation: Two use cases were developed. One that allows Mr Martin to remotely control home appliances, and another that allows Mr Martin to authorize his gas or electricity company to access the home network in order to take a meter reading.

7 IMS Approach for Remote Access

7.1 Overview

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.

The following figure shows a high level architecture over 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 generic IP devices. As UPnP/DLNA [2, 6] can simplify many Remote Access operations, it is considered as a particular case, and the subset of devices that support it are identified in the rest of the document 'UPnP devices'. Remote access to SIP devices in the home is covered by the existing B2BUA functionality in the IMS enabled HG.

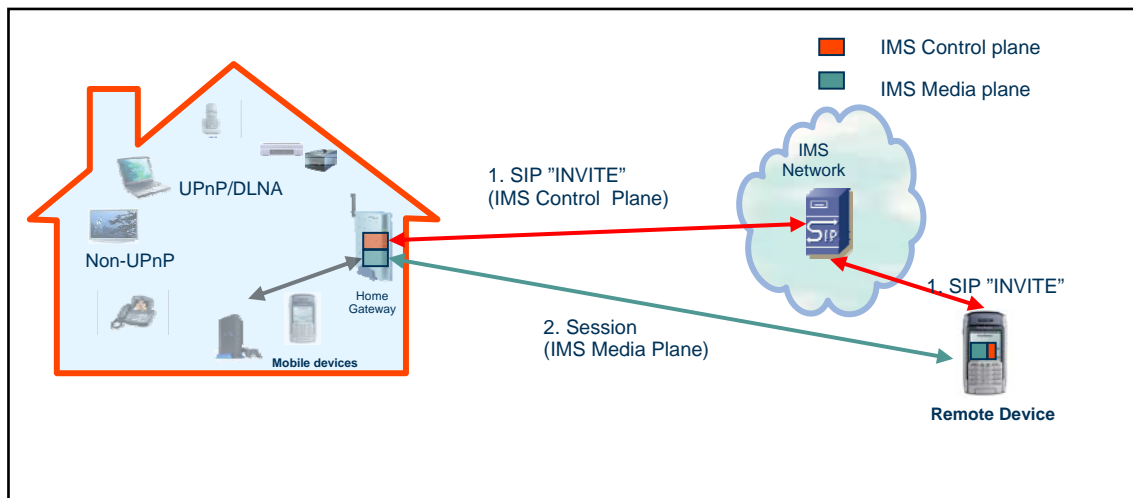


Figure 1 High level IMS based Remote Access Architecture: overview

The principle of “IMS based Remote Access” is that 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 185 005 [3].

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 uploading 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.

7.2 Architecture for IMS based Remote Access

The proposed architecture for an “IMS based Remote Access” uses IMS for setting up a media tunnel against the selected home device. The signaling between the HG and the home device can rely on UPnP [2, 4] or other mechanism. In HGI Residential Profile v1 document [1], the

Remote Access (RA) architecture is shown (in Figure 6, page 32) as a Remote Access block connected to the IMS Interworking block and to the home devices (UPnP and IP).

In Figure 2 below we are focusing to show the architecture for Remote Access from an IMS NGN Remote Device to an UPnP home device as well as an IP home device without UPnP support. In this architectural diagram, four blocks have been included in the new Remote access functionality block:

- RA-Config, ACL Lists: Administrator configuration of ACL's related to Devices
- Device Discovery: Discovery of Home Devices and its services
- Synchronization: Device/Service synchronization between HG and the Remote Device
- Remote Access Transport: Forwarding of traffic between the Remote Device and the Home Device

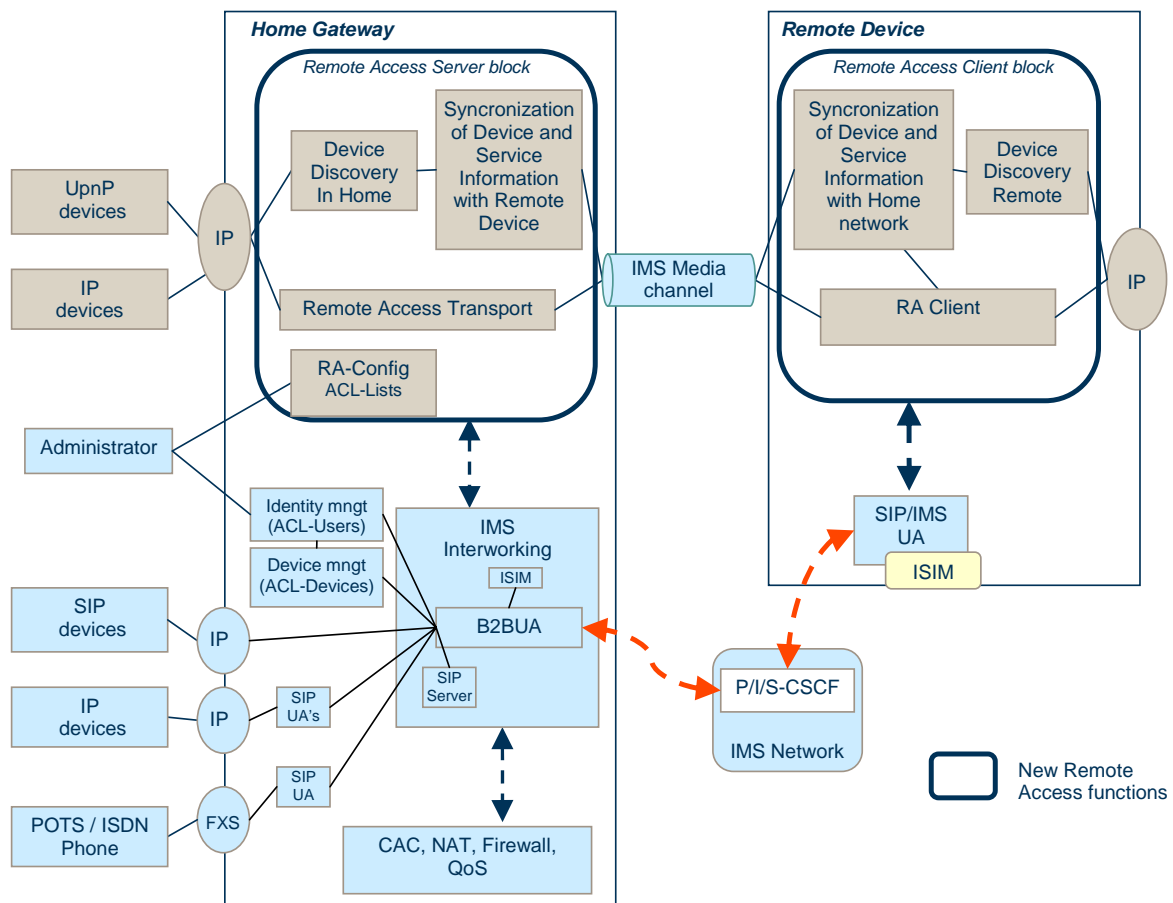


Figure 2 Architectural diagram for IMS based Remote Access

The “blue” boxes are the existing functionality in an IMS enabled HG, as described in section 7.5.2 and shown in Figure 6 in HGI Residential Profile v1 document [1]. The “grey” boxes are the new Remote Access functions needed for enabling secure IMS based remote access. Below follows a summary of the functions/services that relates to IMS and those related to the new Remote access block.

It shall be noted that the Administrator can be either the end-user or the service provider (BSP or ASP). Typically a partitioning into operator managed services and corresponding devices (e.g. Home Automation sub-gateway) and end-user devices is made. The Remote Device can be either an end-user device, a BSP or other application service provider system. One example is an

IMS Application Server for enabling remote access for the end-user also from non-IMS terminals, such as a shared PC on an Internet café.

7.3 IMS Enablers for Remote Access

The role for IMS in the proposed Remote Access scenario can be summarized as follows:

- Routing – IMS network routes via IMS Identities
- Media session setup – IMS media session setup via normal IMS/SIP Invite
- Authentication/Authorization (ACL-Users) – Remote user authorized in HG based on p-asserted-id guaranteed by IMS network (piggy-back on IMS authentication)
- Integrity and confidentiality
 - IMS control plane according to IMS standards
 - Media plane can be defined using key management in SDP negotiation (e.g. according to RFC 4567) [5].
- QoS – QoS managed by IMS and Access networks as for normal IMS media tunnels
- Billing
- Service Provisioning

7.4 Remote Access Functionality in the HG

For Remote Access to home devices, the following functions are needed in the “Remote Access Server block” of the HG in Figure 2.

- Authorization (Devices)
 - Manageable filters for device publication and accessibility
 - ACL-Device: ACL based on IMS identity, UPnP id or other unique device id provided via DHCP for remote control point for each local device
Administrator defines filter for each home UPnP and IP device
 - Manageable filters for remote device visibility in home network
- Synchronization and Device Discovery
 - For device and service synchronization between the HG and Remote Device. As an example UPnP RADA can be used for this synchronization between HG and Remote UE.
 - The “Device Discovery In Home” block collects information over home network devices and services, to be used by the “Synchronization” block.
 - The “Device Discovery Remote” block collects information over remote devices and services, to be used by the “Synchronization” block during the synchronization.
 - The “Device Discovery” blocks also hold functionality to read device information from the HG DHCP server repository.
- Remote Access Transport

- Remote Access signalling and media is transported through the “Remote Access Transport” block in HG. As defined for the IMS HG, the B2BUA (IMS Interworking) controls that the Firewall opens up a pinhole for the remote access media transport.
- The source IP address of the remote media access is also inspected to only allow access to the authorized remote device.

7.5 Remote Access block in HGI IMS Interworking Architecture

In the IMS interworking architecture defined by HGI Residential Profile v1 document [1], the described IMS-approach is indicated as an additional functional block called “Remote Access” as shown in Figure 3 below. The Remote Access block makes use of 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. As already described, the remote access rights on a per IMS user to the local devices are possible to configure in an ACL. The management of the ACL is possible both from the HG end-user as well as the service provider(s). Functionality for the remote terminal to find devices and corresponding services on the LAN is also supported (Synchronization).

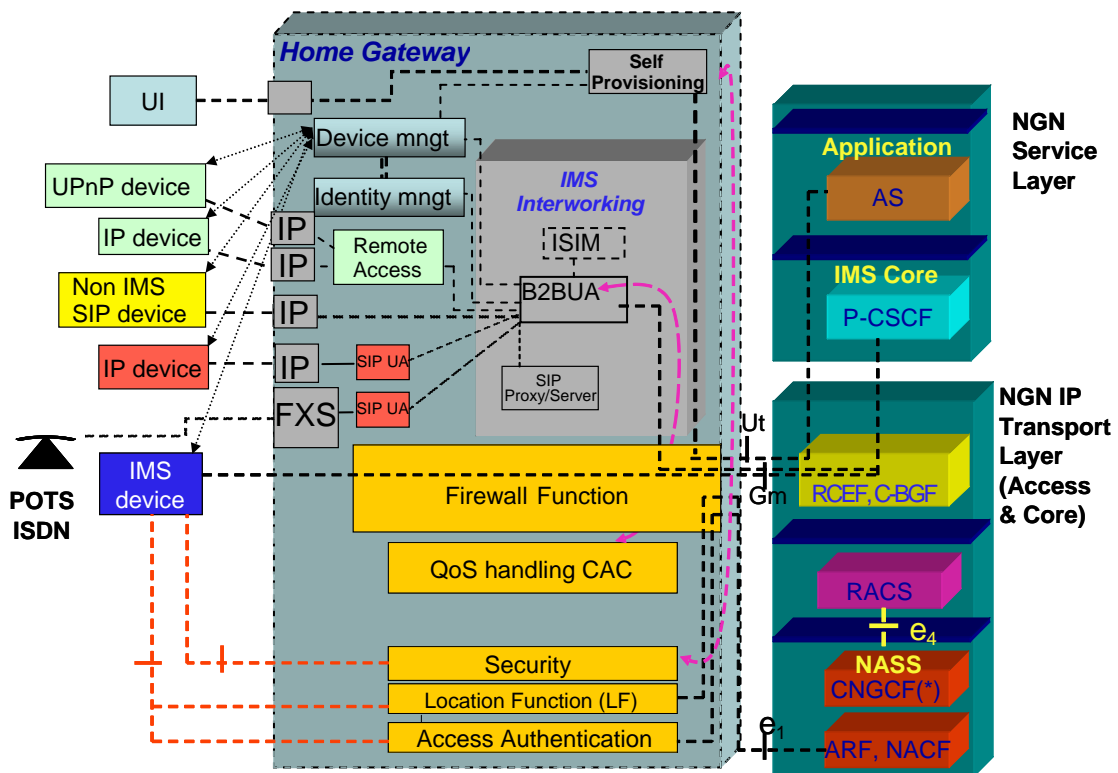


Figure 3 HG functional blocks for interoperability with IMS and NGN core, including the “Remote Access” block.

8 Web Based Approach for Remote Access

For non-IMS based networks the web based approach is defined. It is based on the HG LM Remote UI, which is a web server originally defined for local end-user configuration and graphical user interface. The new requirement is that the web server shall also support SSL/https for remote access.

The ACL is based on user names and passwords for each user (authentication) and their rights of accessing specific end-devices (authorization). Confidentiality for the web server communication is provided using SSL/https.

8.1 Overview

This section outlines an implementation example for the non-IMS based Remote Access.

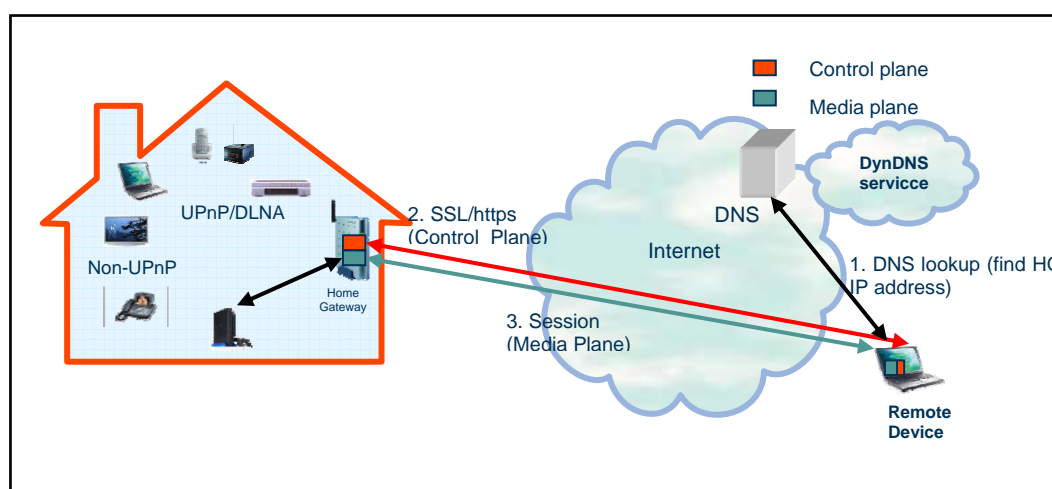


Figure 4 High level Web based Remote Access architecture: overview

The principle of “Web based Remote Access” is that it gives the possibility to use virtually all remote devices with a web browser to remotely access the home. It is based on the HG LM Remote UI, which is a web server originally defined for local end-user configuration and graphical user interface. The new requirement is that the web server shall also support SSL/https for remote access.

Since most of the broadband access solutions are not based on static IP addresses a DynDNS service is needed in order to find the HG with a unique name instead of an IP address. Thus, in this solution the HG is required to support DynDNS client according to HGI v1.0 R249 requirement.

The Remote Device makes a DNS lookup using the HG unique name to find the IP address of the HG. Then it can access the HG web server and log in using his user name and password. Then the secure session is set-up using SSL/https and the remote user can see what devices he is authorized to access. The user can then access a selected device and the media session is established. Encryption of the media session is not a mandatory requirement.

The proposed architecture makes use of the LM Remote UI with SSL/https for controlling the set-up of a media session to the selected home device by opening up a pinhole through the firewall. The signaling between the HG and the home device can rely on UPnP or other mechanism.

The source IP address of the remote media access is also inspected to only allow access to the authorized remote device. [Note! In cases when the remote access is made through a proxy

there are situations when the https traffic and the media session have different IP addresses. In this case the remote device source IP address must be explicitly entered by the user]

9 Operator Controlled Remote Access

An alternative way of providing remote access, which does not put any additional requirements to the HG, is described below. As a representative use case we can take the Home Surveillance and Home Security services which are services delivered over the BSP access network to a specialized Application Service Provider (ASP), in this case a security provider. There is a business agreement between the BSP and the ASP. The solution overview is shown in Figure 5. Note that this is just an example of how the distribution of functionality between the BSP and Security provider can be done. A scenario there the Security Provider also operating the surveillance server, is also possible.

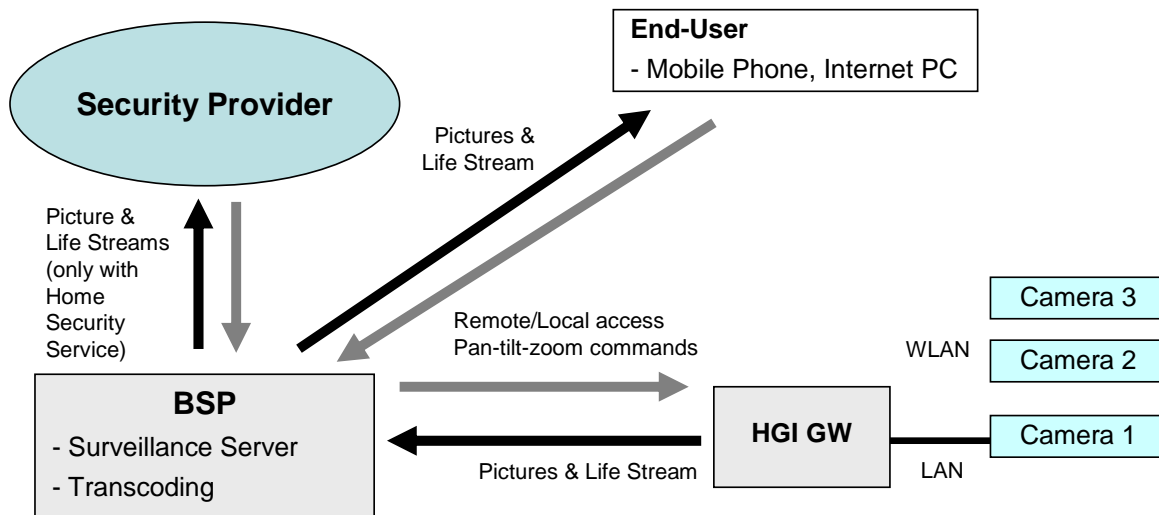


Figure 5 Example of Operator managed Home Surveillance service

Since this is defined to be an operator managed service the requirements from this solution on the HG are about opening up pinholes through the firewall for secure access to a specific end device (camera) from the BSP Surveillance Server (configuration of HG is done from RMS server). The HG does not need to have any specific RA functionality, this means that this is a conceptually different approach than the previous two RA methods (IMS and Web based) described. In this case the ACL is defined as the IP address of the Surveillance Server mapped to the cameras in the home LAN. Confidentiality can be ensured by end-to-end encryption between the camera and the end server. The requirement on the HG is then about supporting multiple VPN through the FW.

As described in section 7.2 the Surveillance Server can also be an IMS application server to offer remote access to non-IMS devices when IMS based Remote Access to the HG is used.

10 References

- [1] Home Gateway Technical Requirements: Residential Profile, Version 1.0.1;
http://www.homegateway.org/publis/HGI_V1.01_Residential.pdf
- [2] UPnP Device Architecture 1.0; <http://www.upnp.org>
- [3] ETSI TS 185 005 TISPAN
- [4] SIP and IMS Residential Gateway, Broadband Europe 2007 conference paper (Tu4A-2)
- [5] RFC 4567; Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)
- [6] Digital living network alliance (DLNA): <http://www.dlna.org/home/>