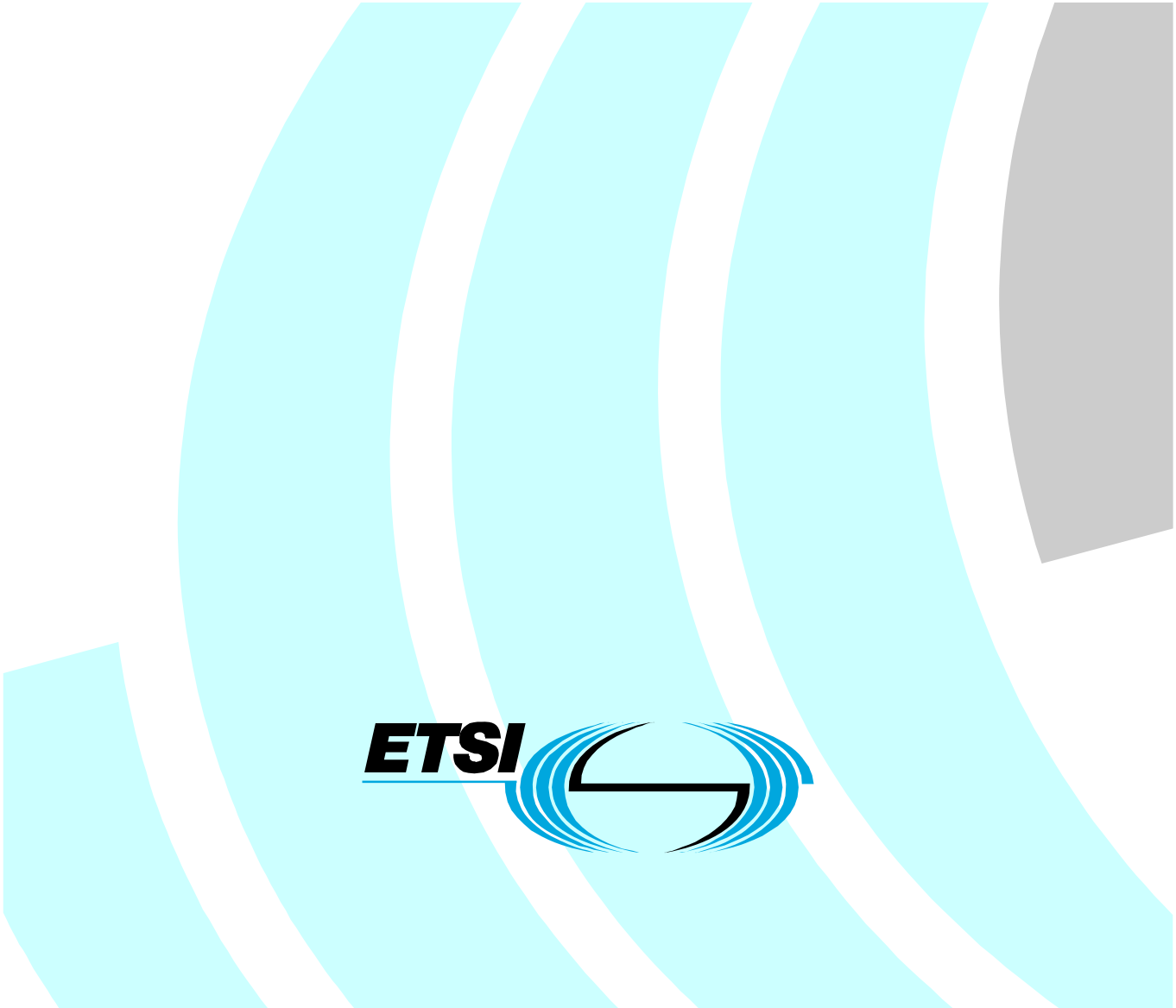
ETSI TS 185 005 V2.0.0 (2007-07)

Technical Specification

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Services requirements and capabilities for customer networks connected to TISPAN NGN



Reference
DTS/TISPAN-05014-NGN-R2

Keywords
gateway, service

ETSI

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

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

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

Contents

Intellectual Property Rights

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

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

Foreword

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

1 Scope

The present document specifies the services requirements and capabilities for Customer Premises Networks (CPNs) and Customer Network Gateways (CNG) connected to a TISPAN NGN as defined in TS 181 005 [1].

Characteristics of Customer Network Devices (CNDs) that can be connected to Customer Networks specified in the present document are addressed.

2 References

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

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

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

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

[1] ETSI TS 181 005: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Services and Capabilities Requirements".

[2] ETSI TS 123 228: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS); Stage 2 (3GPP TS 23.228 Release 5)".

[3] ETSI TS 181 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Direct Communication Service in NGN; Service Description [Endorsement of OMA-ERELD-PoC-V1]".

[4] ETSI TS 181 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Videotelephony over NGN; Stage 1 service description".

[5] ETSI TS 181 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Multimedia Telephony with PSTN/ISDN simulation services".

[6] Home Gateway Initiative: "Home Gateway Technical Requirements: Release 1" http://www.homegateway.org/publis/HGI_V1.0.pdf.

[7] ETSI TS 122 340: "Universal Mobile Telecommunications System (UMTS); IP Multimedia Subsystem (IMS) messaging; Stage 1 (3GPP TS 22.340)".

[8] ETSI TS 187 001: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

3 Definitions and abbreviations

3.1 Definitions

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

Customer Network Device (CND): physical device enabling service(s) usage

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

Customer Network Gateway (CNG): gateway between the Customer Premises Network (CPN) and the Access Network able to perform networking functions from physical connection to bridging and routing capabilities, but also possibly implementing functions related to the service support

Customer Premises Network (CPN): the in-house network composed by customer network gateway, customer network devices, network segments (physical wired or wireless connections between customer network elements), network adapters (performing a L1/L2 conversion between different network segments) and nodes (network adapters with L3 routing capabilities)

NOTE: Other terms used to identify CPN in TISPAN NGN R1 deliverables or outside TISPAN are Home Area Network (HAN), Home or Residential Network, Customer LAN (C-LAN).

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

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

3.2 Abbreviations

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

API	Application Programming Interface
ASP	Application Service Provider
CND	Customer Network Device
CNG	Customer Network Gateway
CoD	Content on Demand
CPN	Customer Premises Network
DLNA	Digital Living Networking Alliance
DNS	Domain Network Service
DRM	Digital Rights Management
FXS	Foreign Exchange Subscriber
HAN	Home Area Network
HTTP Digest	Hyper Text Transfer Protocol Digest authentication
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia PUblic Identity
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPTV	IP Television
ISIM	IMS Subscriber Identity Module
ISP	Internet Service Provider
NBA	NASS Bundled Authentication
NGN	Next Generation Network
P-CSCF	Proxy-Call Session Control Function
PPV	Pay Per View
PSTN	Public Switched Telephony Network
PVR	Personal Video Recording

QoS	Quality-of-Service
SIP	Session Initiation Protocol
STB	Set Top Box
UA	User Agent
UE	User Equipment
UICC	Universal Integrated Circuit Card
VoIP	Voice over Internet Protocol
WAN	Wide Area Network

4 Services requirements and capabilities for customer networks connected to TISPAN NGN

4.1 Service scenarios description

The use cases can be grouped in the following categories:

1) Broadband connection
2) Communication
3) Home worker
4) Home Management and Security
5) Provisioning and Service configuration
6) Entertainment and information
7) Remote Access

4.1.1 Broadband connection

The user wants to access the Internet from a number of PCs at home, and also can decide to subscribe to new services (e.g. parental control, online audio streaming, etc.) offered by his ISP (Internet Service Provider) or an ASP (Application Service Provider), via email or online.

From the service provider point of view, the service must be remotely activated via auto-provisioning, the necessary connectivity including QoS to deliver the service must be guaranteed and there must be the possibility of remotely debugging customer problems.

Figure 1 represents an example for this scenario.

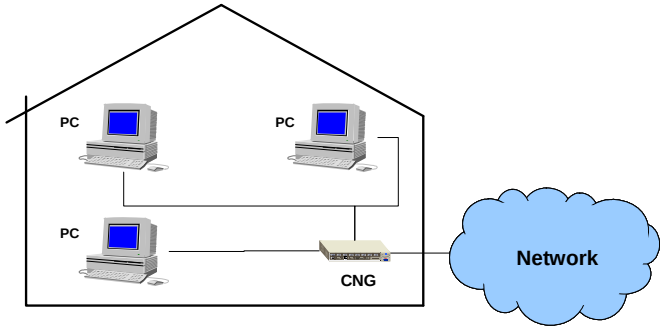


Figure 1: Example of Broadband connection scenario

4.1.2 Communication Services Support

Communication services can be divided at least in three categories:

1) Person-to-Person communication P2P.

2) Person-to-Machine communication P2M.

3) Machine-to-Machine communication M2M.

4.1.2.1 Person-to-Person (P2P) Communication

P2P communication is intended as voice or voice/video communication and it could be performed in three different ways:

- Voice / VoIP with IP phone.
- Voice over IP with legacy analogue phone.
- Video Communication.
- Text communication with legacy text telephone.
- Computer-originated text communication to PSTN.

In the first case, the VoIP phone can be used to make or receive a voice call. In the second, using the voice service is rather easy and is not different from making phone calls via standard PSTN. The supplementary voice services can be used on both lines (call transfer, call hold, etc.) according to the definition of Simulation and Emulation Services in TISPAN. In the third a newly installed video phone can be used to make or receive a video call. The typical supplementary voice services will be available. In the fourth, communication is not different from making a text telephone call via standard PSTN—translation services etc are available. In the fifth, a computer is used as text telephony terminal; when suitable technology is mature, text-to-and-from-voice translation may be done on the computer and a VoIP call made.

The service provider must guarantee the necessary connectivity to deliver the voice, voice/video, or text service, as well as the necessary quality of service.

In the first case, the VoIP phone can be used to make or receive a voice call. In the second, using the voice service is rather easy and is not different from making phone calls via standard PSTN. The supplementary voice services can be used on both lines (call transfer, call hold, etc.) according to the definition of Simulation and Emulation Services in TISPAN. In the third a newly installed video phone can be used to make or receive a video call. The typical supplementary voice services will be available.

The service provider must guarantee the necessary connectivity to deliver the voice or voice/video service, as well as the necessary quality of service.

Figure 2 represents an example of possible implementation for this scenario.

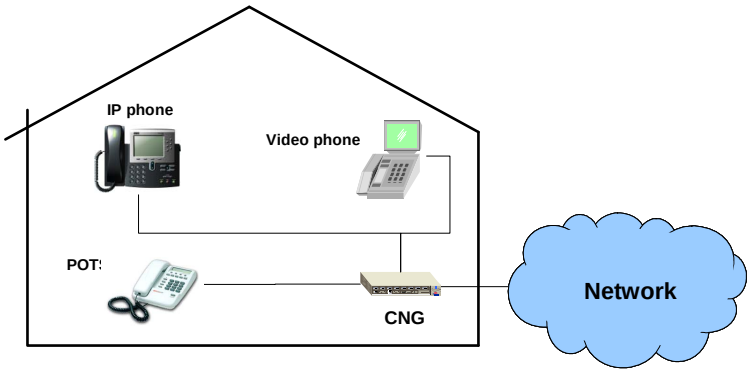


Figure 2: Example of Communication scenario

With specific reference to the personal communication services, the possibility to use one identity on several terminals as well as to share one terminal with several identities should be supported. In these cases, the Customer Network Gateway could play an active role, according the technical solution chosen.

For example it should be possible to use a unique shared public identity (a family identity) to make a call with one of the terminal at home. When the call is direct to the shared public identity all the terminals at home ringing because they are associated at the same shared public identity. Moreover each terminal may have its own public identity (different from family identity) so a call can address directly to it. Figure 3 shows the "shared IMPU" use case as also described in TS 123 228 [2].

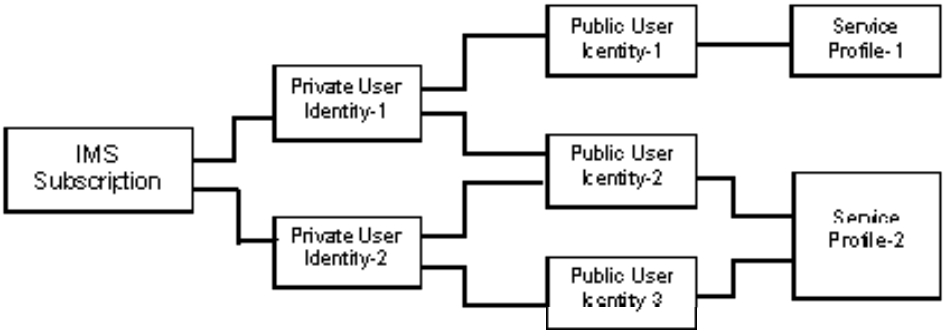


Figure 3: Shared public identities use case

4.1.2.2 Person-to-Machine (P2M) Communication

A typical P2M communication use case is, for example remote access of device, where one can access the home media server for uploading or downloading one's photos remotely, that is mentioned in the remote access service section.

4.1.2.3 Machine-to-Machine (M2M) Communication

One of the typical use cases for M2M communication from the customer network and NGN standpoints is the automatic electricity meter reading business. The electricity meter is a CND that is attached to the CNG, and the electricity charging server is an IMS enable device that is connected to the NGN service layer. With this approach, network operators can reuse the NGN security functions in CNG and electricity charging server for delivering secure data service between customers' electricity meters and electricity companies' charging servers (that can be hosted by the operator, IT provider or the electricity company itself depending on the business model).

4.1.3 Home worker

In this use case various members of a family simultaneously use the broadband infrastructure. In particular, parents are connected to their respective corporate intranets over a secure link and perform a number of actions, including upload and download of documents, placing VoIP calls for work. They expect to have a simple mechanism by which they can easily switch from private to corporate calls (billing will be different). While the parents are working, children must be able to watch video streaming, or browse the Internet. All these simultaneous applications have to live up to the experiential expectations of the user. Hence the necessary priorities have to be taken into account within the customer network environment.

4.1.4 Home Management and Security

Two different sub cases are proposed for this category: the first is related to the access/parental control, the second to the personal monitoring.

4.1.4.1 Access control

The user wants to be sure that she has an overview on the children communication and entertainment activities and be able to control the access to these activities. An access control service can be built up with the following capabilities: Content check, Cost check, Usage check, Time check. The user must have the capability to check the configuration of the access control service via a terminal (e.g. a PC) and changes of the parental control configurations can be only performed by himself as administrator.

From the service provider point of view, a number of mechanisms for service activation, billing and web based consumer support in case of problems must be ensured.

4.1.4.2 Personal Monitoring

In this use case the user must be able to access images coming from a camera installed at home, via an Internet browser on a remote PC or/and via a mobile Internet connection. Fast internet access with Wi-Fi service is enabled in the house and IP Camera has a build-in web server and can act PC independent. The camera must have an indicator showing when it is active, perceivable even if only a single image is transmitted. No fixed IP address is required to remotely access the camera (Dynamic DNS service included). A security mode can allow the camera to react on motion detection and send an alert via an e-mail to one or more addresses with a few seconds of images attached, or via SMS.

The service provider must ensure the actual reachability of the camera installed at home, even if the installation has been performed directly by the user himself.

4.1.5 Provisioning and service configuration

A set of parameters shall be configured on UE (device that contains the SIP UA) to access to IMS network. These parameters should be provisioned on UE in order to make seamless for the user the UE registration to IMS network (enabling UE automatic registration on start-up procedure). In addition, they should be "portable", thus meaning that user can assign his/her public identity (and the associated parameters) to a different UE. In case the UE is loaded with UICC both requirements are satisfied:

Use Case: First Provisioning (Manual)

- The user has a new device.
- The user subscribes an IMS service.
- Network Operator provides the user with the information needed to access to IMS network through an off-line channel (i.e.: by e-mail, fax, etc.).
- The user fills in manually the configuration parameter fields on his/her device with needed information to access to the IMS network (e.g. IMPU, IMPI, Shared keys, Home Network Domain or P-CSCF IP Address, etc.).
- This kind of customer experience may be suitable for softphone, but it's quite difficult on a hard phone.

Use Case: First Provisioning (automatic)

- The user has a new device.
- The user subscribes an IMS service.
- A Network Configuration Service must be able to send configuration parameters to access to the IMS network (e.g. IMPU, IMPI, Shared keys, Home Network Domain or P-CSCF IP Address, etc.), to the CND when the user starts up the device.
- No manual insertion by the user is needed.

Use Case: Manual Re-Configuration

- The user is already using a specific device associated to a specific public identity. He wants/needs to:
  - use a different device with the same public identity, or
  - assign a different Public Identity to the same device.
- As for the previous case relative to the provisioning phase, the user can manually configure the device with the public ID and the associated configuration parameters.
- If the user wants/needs to use the same parameters (public identity, username and password) on a different device, the CND to which these parameters have been previously assigned shall be deregistered, in order to de-assign association device-configuration parameters.

Use Case: Self Re-Configuration Service

The user is already using a specific device associated to a specific public identity. He wants/needs to:

use a different device with the same public identity, or

assign a different public identity to the same device.

- The user accesses a Self Configuration Service through a web interface and/or device-specific menus, to:
  - Select the device to which assign the public identity and the associated IMS configuration parameter.
  - Select the public identity, and the associated configuration parameter, to be assigned to a specific device.

Based on user' s selection the device is automatically configured by the network.

4.1.6 Entertainment and information

A number of different use cases can be proposed for this category. Here three specific scenarios are proposed, the first related to the broadcast IPTV service usage inside the house, the second to the access to contents stored in a media gateway, the third to gaming scenarios.

4.1.6.1 IPTV - Broadcast TV Service

The user is able to view access channels and other content from his broadcast IPTV service using his television connected to this set-top-box. A TV is directly connected to the STB. The STB is intended as separate device not integrated in the CNG. It is assumed that in most cases the television is directly connected to the set-top box. Also, he The user may choose to have a range of viewing devices within the home, not just a single television directly connected to the set-top-box so that family members should be able to view the broadcast IPTV channels and other content from any compatible viewing device within the customer network. The user expects that the IPTV streams within the house will provide a quality picture and experience, so appropriate bandwidth must be dynamically available through the customer network. Figure 4 represents an example of this scenario.

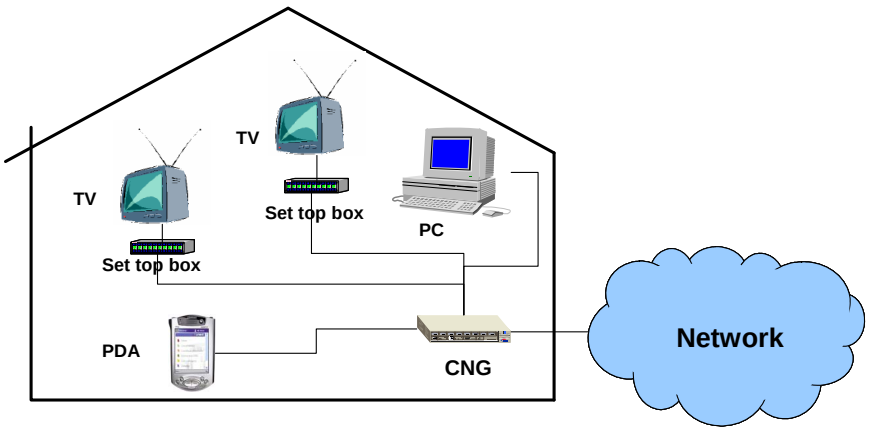


Figure 4: Example of IPTV - Broadcast service

Considering the different situations in terms of service features and type of devices used the IPTV customer scenarios can be categorized in the following way:

- "Basic" IPTV usage: media streaming with zapping possibilities (same user experience as for the traditional terrestrial TV): single stream on a CND (i.e. STB connected to a TV).
- "Advanced" IPTV usage: media streaming with PVR functionalities (time shifting, video recording etc.), single stream on a CND (i.e. STB connected to a TV)
- "Nomadic" basic or advanced IPTV service, including the possibility of redirecting the media flow from a device to another in the CPN environment (but always single stream on CND).
- "Multi device" scenarios: single stream usage on multiple devices, either with basic or advanced features. Advanced features should be applied to all connected CND. Single/Multi room situations are included in this scenario, with possible different issues in terms of pure connectivity and QoS (especially when a wireless technology is used).
- "Multi service" scenarios: usage of broadcast IPTV + additional concurrent services on the same device (typically, communication services as defined in TS 181 016 (see bibliography): direct communication as in TS 181 006 [3], immediate messaging as described in TS 122 340 [7], notification of incoming calls related to Videotelephony and multimedia telephony services as described in TS 181 001 [4] and TS 181 002 [5]. "Multiple" scenarios allowing multiple IPTV streams on multiple CNDs with basic or advanced functionalities and with or without concurrent services.

4.1.6.2 On demand IPTV services

In addition to the broadcast TV flows, the usage of contents that are available upon a specific request user side must be considered. Following the contents of TS 181 016 (see bibliography) this can be performed in different ways:

- *Pay Per View (PPV)*: the user can ask for being authorized to have access to a specific content, whose schedule is defined by the service provider, without any specific possibility of interacting with the flow itself (it will be seen as the typical live TV streams).
- *Content on Demand (CoD)*: the user can ask for having access to a specific content, with the possibility of controlling when and how it is viewed. It includes the possibility of performing pause, rewind, forward actions on the media flow. A "near CoD" and "push CoD" versions of this service are limiting in some way the possibility of direct intervention user side (mainly about timing) or providing a time separation between the content download and the actual usage phases.
- *Interactive TV*, providing additional bidirectional information flows typically associated to the broadcast IPTV service usage. These information flows can allow the user performing specific actions (for example, voting), ask the user for performing actions (e.g. payment overdue notice) or be simply informational.

All these services will be based on an interaction between the CPN and some servers placed in the NGN; specific functionalities must be provided in the customer network gateway and customer network devices, but there can be the possibility of implementing specific functionalities on a separate hardware performing storing, possible transcoding and/or protocol adaptation: this kind of device can be identified as "media gateway" or "application gateway".

4.1.6.3 IPTV services based on presence

A particular case mainly related to the usage of broadcast IPTV contents is the interaction between IPTV and presence information. As defined in TS 181 016 (see bibliography) presence information can be used to optimize specific basic or additional services related to IPTV (for example, personalized EPG and advertising, parental control etc). This must be taken into account when depicting the CPN related requirements from what the CNG and STB functionalities will be derived.

4.1.6.4 Gaming

The user can have access to some game application installed in devoted (i.e. game consoles) or general purpose devices. This can require a connection to a game server or a peer game devices and involves some requirements in terms of user experience (corresponding to low delay and latency from a technical point of view). Also, a number of concurrent applications can be used, for example messaging tools can be used or VoIP sessions can be established in parallel, to allow the users sharing opinions and information during the service usage. Customer devices used for gaming can be mobile and so they can join different customer networks depending on the user's needs.

4.1.7 Remote Access

When a user is away from its customer network, it is in many situations valuable to be able to access services on the customer network. Remote access can be divided into two categories: access of devices and access of services. Example of first category is uploading the latest vacation pictures or films to a storage server on the customer network or when a user sends a message to the home to turn on/off a device. Example of the second category includes accessing a surveillance camera service to check that everything is in order. A use case in the same theme may be when the end-user accesses content stored on its customer network while being away at a friend's house or similar. Another, more futuristic, use case may be when an end-user wants to access its subscribed broadcast media channels when away from its customer network(s).

The CNG shall provide secure access control and connectivity to the customer network, assisted by standard NGN functions. The customer network may be reached from the open Internet, but by accessing it through the operator managed IMS/NGN, where for example NGN-assisted QoS can be applied for critical parts of the network path, an enhancement of the end-user experience may be achieved. Figure 5 outlines the remote access use case, exemplified with the DLNA concept.

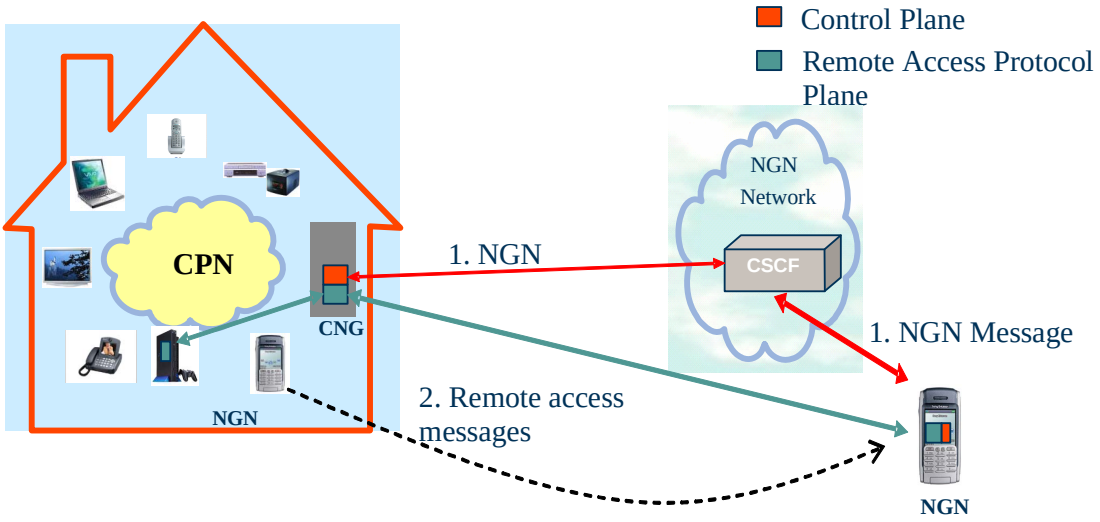


Figure 5: Schematic view of Remote access architecture

4.2 Overview of terminals/equipment supported

The overview of possible equipment to be considered is contained in TS 185 006 (see bibliography).

4.3 Requirements derived from service scenarios

A number of detailed requirements for the customer networks can be derived from the use case illustrated in the previous clauses.

Requirements are split in:

- General requirements on Customer Network Gateway.
- General requirements on Customer Devices.

- Specific Requirements for communication services support.
- Specific Requirements for entertainment and information services.
- Specific security requirements.
- Specific QoS requirements.
- Specific management requirements.

4.3.1 General Requirements on Customer Network Gateway

1) The CNG shall be equipped with a WAN interface towards the NGN, implementing layer 1 and 2 functionalities ("one-box" solution).

2) LAN interfaces. The CNG shall be equipped with at least one Ethernet (minimum 100 Mbit/s) is interface. Optional interfaces could be present, e.g.: wireless LAN Wi-Fi Alliance certified, Powerlines, Plastic Optical Fiber, USB device and/or host, one or more FXS for analog telephony, DECT Cat-iq.

3) The CNG shall support both routed and bridged modes of operation.

4) The CNG shall support direct intra-LAN connectivity between any appropriate pair of devices on the Customer Premises Network.

5) The CNG shall support different IP address schemes and subnets on the same physical LAN port, and on different LAN ports, irrespective of routed or bridged mode of operation, allowing the direct addressability of CNDs from the NGN side in relation to data plane, control plane and management plane flows.

6) The CNG and devices shall support mechanisms to identify and share information about the customer network devices (e.g. type of device and basic capabilities, services supported etc.) within the customer environment. Some of this information can be used locally, while a subset of it can be forwarded to the NGN.

7) The CNG shall support use of one user identity on several terminals as well as to share one terminal with several identities.

8) The CNG and the Customer Network shall support the NGN services usage (e.g. voice communications, video communications, IPTV, entertainment, …) allowing the connection to the right service control platforms.

9) The CNG should support or not prevent redirection of IP Multimedia sessions, as defined by TS 181 005 [1], independently from the type of device used (NGN terminal or other CND).

10) The CNG and the Customer Network shall assure the confidentiality, the integrity of signalling/control/media and management flows.

11) The CNG and the Customer Network shall provide the opportunity for a customer network administrator to perform service and network-related configuration. According to the service/network provider choices, the CNG and Customer Network may prevent - user initiated modification of network and service related parameters.

12) The CNG should negotiate session parameters (bandwidth, screen resolution, codecs…) with the NGN transparently to the user.

13) The CPN shall support secure remote access control, based on NGN network functions.

14) The CNG shall allow the customer remote access to a CND in the Customer Network, for example a surveillance video camera.

15) Standard NGN authentication, routing and connectivity should be used to establish remote access connectivity.

16) The CNG may allow secure dynamic firewall opening for remote access devices based on NGN authentication functions.

17) The CPN may support encrypted communication with remote access devices, and the encrypted communication can be terminated either at the CNG or CND.

18) The CNG may act as a proxy for handling messages (requests and responses) related to the remote access scenarios to and from the home.

19) The CNG may support mechanisms supporting nomadism of the users and their subscribed services from one physical customer environment to another.

4.3.2 General requirements on Customer Network Devices

20) A CND, as defined in clause 3, may use the CNG to access NGN services.

21) Authorized users shall be able to access NGN-based services using any NGN supported home device.

22) Both IMS capable devices with or without UICC and non-IMS capable devices without UICC shall be supported.

23) If the CND contains an ISIM/UICC, it shall support the AKA authentication method (TS 187 001 [8])

24) If the CND does not contain an ISIM/UICC, it shall support the HTTP Digest authentication or the NBA (TS 187 001 [8]).

25) The CND shall provide its private identity, when it requires the registration to the network.

26) In order to support the NGN services and intra-CPN communications, all the CNDs in the CPN shall be addressable directly or by the mean of the CNG using L2/L3 mechanisms.

27) The CND should support protocols for remote access management.

28) The CND should support protocol for local authentication in CPN/CNG.

29) The CND shall support protocols to process the media.

30) The CND shall support protocol to access the NGN service layer platforms.

31) The CND shall support protocols to access Self Configuration application (as defined in clause 4.1).

32) The CND shall be able to download and install client application services.

33) The CND should be able to communicate its services related capabilities to the CNG.

34) The CND should be able to support one or more codecs for communication services (as defined by TS 181 005 [1]).

4.3.3 Specific Requirements for communication services support

35) Multiple identities should be supported within the same subscription. Personal service profiles per each identity within the same subscription should be supported. A shared public identity on several terminals, with different private identities, shall be supported (shared IMPU).

36) Multiple public identities on the same terminal shall be supported.

37) The CNG shall support a mechanism allowing the support of call forking towards customer non-IMS capable devices and shall able to store information related to private identities of non-IMS capable CNDs.

38) The CNG shall support a mechanism allowing the support of call forwarding toward non-IMS capable CNDs.

39) The CNG shall support intra-CPN communication between IMS and non-IMS capable CNDs.

40 The customer environment (CNG and/or CNDs) should support a mechanism to allow service roaming (i.e. using the same CND in two different CPNs declaring the same public identity). Supporting this scenario for non IMS capable CNDs is still to be discussed.

41) The NGN network should be provided with a CND location information.

42) Codec requirements and capabilities for the User Equipment (including the CNG) are already defined in TS 181 005 [1] which describes service requirements and capabilities for the TISPAN NGN.

4.3.4 Specific Requirements for entertainment and information services

43) The CNG shall support mechanisms for managing IPTV flows provided both in unicast and multicast mode.

44) In case of multicast flows the CNG shall keep a record of which devices are subscribed to which multicast group.

45) An IPTV media flow shall be terminated by a STB or by a specific device called "media gateway" (or "application gateway"). The CNG shall not terminate any IPTV flow by itself.

46) The CNG shall support the connection to a STB (or media gateway) both in a bridged or in a routed mode of operation.

47) Depending on the operation mode chosen (bridged or touted) and on the type of flow treated (unicast or multicast) the CNG shall forward packets only to the physical interfaces which are connected to devices interested to the IPTV flow.

48) In case of multicast streams the CNG should support proxy functionalities to optimize the management of information related to signalling.

49) CNG shall perform a link layer multicast to unicast translation if the STB or media gateway are connected using customer network technologies not supporting multicast flows (e.g. powerlines, wireless).

50) STB or media gateways should be equipped with a programmable open API allowing the implementation of specific service logics.

51) Functionalities related to Electronic Programming Guide and DRM management shall be implemented in STB or media gateway and not in CNG.

52) Media flows (data plane) transcoding shall be performed by STB or media gateway and not by the CNG.

53) Protocols adaptation for control plane or management plane may be performed by CNG.

54) Presence related information shall be sent to the NGN by the STB or the CNG (depending on the specific architectural choices, CNG could manage the presence related information on behalf of the specific device used) to enable specific services tailored on the specific user's profile.

4.3.5 Specific Security requirements

55) The CNG shall support mechanisms to authenticate itself to the NGN for connectivity purposes.

56) The CNG shall support mechanisms to authenticate itself to the NGN for service usage purposes.

57) The CNG shall support mechanisms to authenticate CNDs to the NGN for service usage purposes if they are not able to fully support the related procedures in an autonomous way.

58) The CNG shall support mechanisms for authentication of wireless CNDs for local connectivity. Similar mechanisms may be also implemented for non-wireless devices.

59) The CNG and CPN shall support mechanisms that prevent access to the network by unauthorized users.

60) The capacity of the authorized entities should depend on the security policies defined by the service providers, managing the CNG.

61) The CNG and the CPN shall implement mechanisms to limit the visibility of the WAN side network and resources to authorized entities.

62) The diagnostic operations on the CPN by an operator shall be performed in accordance with rules protecting the users' privacy.

63) CPN environment shall be protected with a stateful firewall function, that may be implemented in the CNG.

64) The CNG and the CPN shall be able to support parental control related functionalities limiting the use of the broadband connection on a user or time basis. Limitations on a content basis may be shared with devoted network servers.

4.3.6 Specific QoS requirements

65) The CNG and the CPN shall support adequate Quality of Service mechanisms (e.g. prioritize the traffic in the event that there is not sufficient bandwidth in the customer network in order to ensure the correct network performances to each traffic flow). To achieve this objective a number of functionalities shall be supported by CNG and/or CNDs, as defined in the following bullets. The following set of requirements is defined adopting as a reference the Home Gateway Initiative (HGI) Release 1 Specification mentioned in clause 2 [6].

66) The NGN network QoS functions shall be possible to use to enhance the end-user experience.

67) The CNG shall classify packets entering the CPN through its WAN interface (downstream direction) according to a number of predefined priorities. Classification can be done on the basis of different layer 2 and/or layer 3 parameters.

68) The number of possible values defining the packet priority and, by consequence, the number of queues managed in the downstream direction shall be coherent with the number of concurrent services (data, communication, entertainment) to be treated and supported.

69) When forwarding packets from the WAN interface to the customer network, the CNG shall perform one of the following three actions, depending on the classification results: manage a number of queues corresponding to the different priorities detected in the classification phase for each packet processed, send the packets to some internal buffers or simply drop the packet.

70) The CNG shall classify packets coming from the CPN through its LAN interfaces (upstream direction) according to a number of predefined priorities. Classification can be done on the basis of different layer 2 and/or layer 3 parameters.

71) The number of possible values defining the packet priority and, by consequence, the number of queues managed in the upstream direction shall be coherent with the number of concurrent services (data, communication, entertainment) to be treated and supported.

72) When forwarding packets from the customer network to the WAN interface, the CNG shall manage a number of queues corresponding to the different priorities detected in the classification phase for each packet processed.

73) The CNG shall be able to classify intra-LAN traffic that is simply bridged by the CNG itself within the CPN.

74) Traffic marking: depending on what are the parameters used to perform classification, CNDs or CNG itself on behalf of the CNDs shall be able to modify the packets' priority.

75) In case of huge amount of traffic in upstream or downstream directions, a congestion management mechanism shall be implemented in the CNG to minimize the impact from the user experience point of view.

76) In case of managed services, QoS rules applied by CNG shall be configurable by a remote management system.

77) In case of unmanaged services, user shall be able to access a QoS configuration function implemented in the CNG.

4.3.7 Specific Management requirements

78) CNG shall be equipped with an application client to be remotely manageable by the service providers for configuration, monitoring, firmware upgrade purposes. In case of multiple service providers multiple clients configuring different sets of parameters (for example referring to different services) may be present. A single parameter can be modified by a single client only.

79) It shall be possible to configure the CNG (e.g. firmware downloading) according to the subscribed services. This operation may be performed when the CNG is connected to the network for the first time, for each new service subscription/modification, or for any technical management (e.g. security, patches, etc.).

80) CNG shall support mechanisms for secure authentication and communication with the remote management system.

81) The CNG shall be associated with a unique Hardware ID to be used for identification NGN side.

82) In case of managed services, the CNG shall support zero-touch provisioning to activate new services, starting from Internet access to voice and video services and shall be remotely manageable. In case of unmanaged services the user shall be able to configure the CNG by himself.

83) The CNG Remote Management requires to manage a specific set of parameters. At least the following list of parameters shall be available: Customer Identification, Physical Line Identification, list of subscribed services, CNG IP address.

84) For the CNG management it is recommended to use a single protocol, so as to minimize the complexity and the cost of the service.

85) CNDs connected to the CPN and devoted to specific managed services shall be remotely manageable (e.g. VoIP phones, Video phones, STBs, etc).

86) CNG shall support mechanisms allowing the CNDs remote management when applicable.

87) Protection mechanisms shall be implemented to avoid that a management client could access and modify parameters that is not allow to configure.

88) The CPN (trough CNDs and/or CNG) shall support manual configuration to insert information to access IMS network (e.g. IMPU, IMPI, Shared keys, Home Network Domain or P-CSCF IP Address, etc.).

89) The CND directly or through the CNG must be able to access to Network Configuration Service Function avoiding any user interaction. (and so the Network Configuration Server should be able to upload different parameter related to service subscription).

90) The CND should be able to support bootstrap capabilities in order to retrieve network configuration data to connect the NGN.

91) The CND/CNG shall support a mechanism allowing the user to manually modify the association between a public identity (e.g. phone number) and a specific private identity corresponding to a single customer device not provided with a UICC.

92) The CPN (CND and/or CNG) shall support a method to access a Self Configuration Server.

Annex A (informative): Bibliography

ETSI TS 185 006: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN Customer Devices architecture and interfaces".

ETSI TS 181 016: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Requirements to integrate NGN services and IPTV".

History

Document history		
V2.0.0	July 2007	Publication