OIPF

Functional Architecture

[V1.2]-[2008-12-08]

Open IPTV Forum

Open IPTV Forum

Postal address

Open IPTV Forum support office
650 Route des Lucioles
06921 Sophia Antipolis
FRANCE
Tel.: +33 4 92 94 43 83
Fax: +33 4 92 38 52 90

Internet
http://www.oipf.tv

Disclaimer

The Open IPTV Forum members accept no liability whatsoever for any use of this document.

Copyright Notification

Content

Figures

Tables

1. Scope (Informative)

The Open IPTV Forum has developed an end-to-end solution to allow any consumer end-device, compliant to the Open IPTV Forum specifications, to access enriched and personalized IPTV services either in a managed or a non-managed network.

To that end, the Open IPTV Forum focuses on standardizing the user-to-network interface (UNI) both for a managed and a non-managed network, as depicted in Figure 1-1.

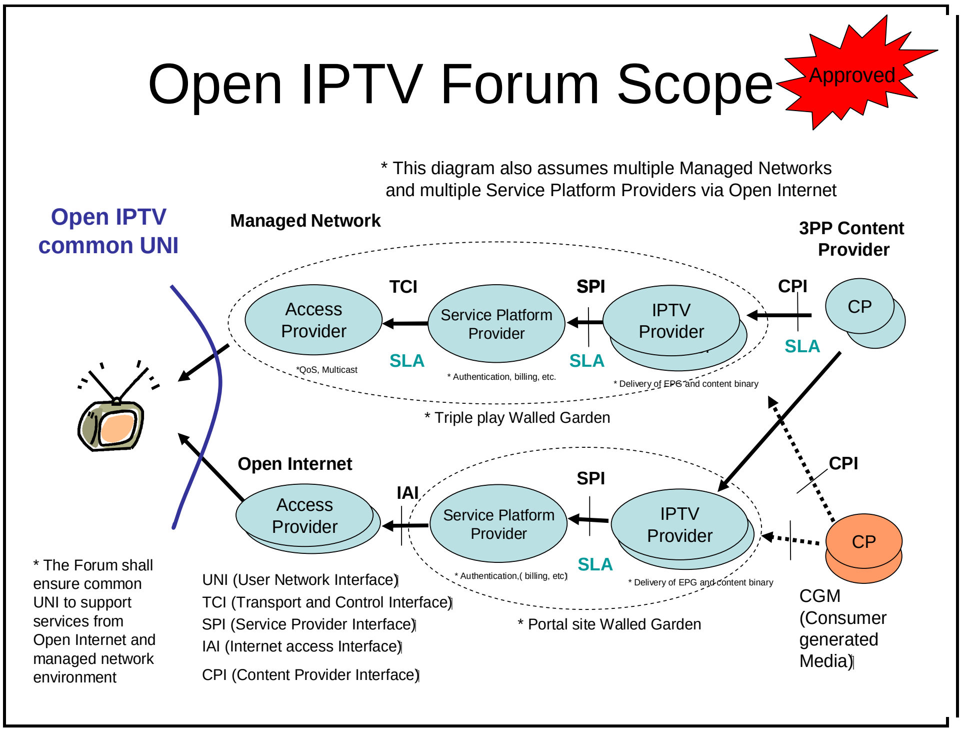

Open IPTV Forum Scope
Approved
* This diagram also assumes multiple Managed Networks and multiple Service Platform Providers via Open Internet
Open IPTV common UNI
Managed Network
3PP Content Provider
TCI
SPI
CPI
Access Provider
Service Platform Provider
IPTV Provider
CP
SLA
SLA
SLA
*QoS, Multicast
* Authentication, billing, etc.
* Delivery of EPG and content binary
* Triple play Walled Garden
Open Internet
IAI
SPI
CPI
Access Provider
Service Platform Provider
IPTV Provider
CP
SLA
* Authentication,(billing, etc)
* Delivery of EPG and content binary
* Portal site Walled Garden
* The Forum shall ensure common UNI to support services from Open Internet and managed network environment
UNI (User Network Interface)
TCI (Transport and Control Interface)
SPI (Service Provider Interface)
IAI (Internet access Interface)
CPI (Content Provider Interface)
CGM (Consumer generated Media)

Figure 1-1 Open IPTV Forum scope

Throughout this document, the terms “Open Internet” and “Unmanaged Network” are used interchangeably, to refer to the ability to access any Service Provider using any Access Network Provider without any quality of service guarantees.

2. References (Informative)

[Ref 1]	DSL Forum TR-069, “CPE WAN Management Protocol”
[Ref 2]	DLNA Networked Device Interoperability Guidelines, October 2006
[Ref 3]	CEA-2014, Web-based Protocol and Framework for Remote User Interface on UPnP™ Networks and the Internet (Web4CE)
[Ref 4]	ETSI TS 102 034, “Transport of MPEG-2 TS Based Services over IP Based Networks”
[Ref 5]	Ethernet Priority, IEEE Std. 802.1Q-2003, “Virtual Bridged Local Area Networks”
[Ref 6]	IETF RFC 2475, “An Architecture for Differentiated Services”.
[Ref 7]	IEEE 802.11, Wireless Local Area Networks
[Ref 8]	IETF RFC 4541, “Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches”, May 2006
[Ref 9]	IETF RFC 4605, “Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP/MLD Proxying")”
[Ref 10]	IETF RFC 3376, “Internet Group Management Protocol, Version 3”, October 2002
[Ref 11]	IETF RFC 4608, “Source-Specific Protocol Independent Multicast in 232/8”, August 2006
[Ref 12]	ETSI ES 282 003, “Resource and Admission Control Subsystem (RACS)”
[Ref 13]	ETSI TS 102 539, “Carriage of Broadband Content Guide (BCG) information over Internet Protocol (IP)”
[Ref 14]	IETF RFC 3550, “RTP: A Transport Protocol for Real-Time Applications”
[Ref 15]	3GPP TS 23.228, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2”
[Ref 16]	IETF RFC 2617, “HTTP Authentication: Basic and Digest Access Authentication”
[Ref 17]	3GPP TS 33.203, “3G security; Access security for IP-based services”
[Ref 18]	3GPP TS 24.229, “IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP)”
[Ref 19]	IETF RFC 2326, “Real Time Streaming Protocol”
[Ref 20]	ITU-T Recommendation E.164, “The international public telecommunication numbering plan”
[Ref 21]	IETF RFC 3261, “The session initiation protocol”
[Ref 22]	Open Mobile Alliance “Instant Messaging using SIMPLE” (OMA-ERP-SIMPLE_IM-V1_0-20070816-C)
[Ref 23]	ECMA-262, “ECMAScript Language Specification”, 3rd edition, December 1999.
[Ref 24]	Open Mobile Alliance “Presence SIMPLE Specification” (OMA-ERP-Presence_SIMPLE-V1_0_1-20061128-A)
[Ref 25]	3GPP TS 33.220, “Generic Authentication Architecture (GAA); Generic bootstrapping architecture”
[Ref 26]	3GPP TS 29.228, “IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents”
[Ref 27]	3GPP TS 32.225, “Telecommunication management; Charging management; Diameter charging applications”
[Ref 28]	UPnP Forum, “UPnP Device Architecture Version 1.0”, June 13, 2000.
[Ref 29]	DSL Forum TR-104, "DSLHome™ Provisioning Parameters for VoIP CPE"
[Ref 30]	DSL Forum TR-135, Working Text 135 "Data Model for a TR-069-enabled STB"
[Ref 31]	DSL Forum TR-140, "TR-069 Data Model for Storage Service Enabled Devices"

[Ref 32]	IEC 62455, "Internet protocol (IP) and transport stream (TS) based service access"
[Ref 33]	DSL Forum TR-098, “Internet Gateway Device Version 1.1, Data Model for TR-069”
[Ref 34]	Java Community Process, Java Specification Request 218 “Connected Device Configuration (CDC) 1.1”
[Ref 35]	ETSI ES 282 003 V2.0.0 (2008-05), ETSI Standard, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-System (RACS).

3. Terminology and Conventions (Normative)

3.1 Conventions

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

Term	*Definition*
Access Network	The network infrastructure used to deliver IPTV services to the Consumer. The Access Network infrastructure (which may include the Internet) is used for the delivery of the content and may include quality of service management to ensure that appropriate network resources are available for the delivery of the content.
Application	Collection of assets and logic that together provide a Service to the User. Assets and logic may reside either in an application Server or in the ITF or both.
Consumer domain	The domain where the IPTV services are consumed. A consumer domain can consist of a single terminal or a network of terminals and related devices for service consumption.
Consumer Network	The local area network in which the IPTV Terminal Function is located. Consumer Networks include residential networks, hot spots, hotel networks etc.
Consumer(s)	See End User(s).
Content	An instance of audio, video, audio-video information, or data.
Content Guide	An on-screen guide to Scheduled Content and Content on Demand, allowing a User to navigate, select, and discover content by time, title, channel, genre, etc.
Content on Demand (CoD)	A Content on Demand service is a service where a user can select the individual content items they want to watch out of the list of available content. Consumption of the content is started on user request.
Content Protection	Means to protect content from unauthorized usage such as re-distribution, recording, playback, duplication etc
Content Provider	Entity that provides Content and associated usage rights to the IPTV Service Provider.
End User(s)	The individual(s) (e.g., members of the same family) who actually use the IPTV Services.
Internet	The Internet is the worldwide, publicly accessible network of interconnected computer networks that transmit data by packet switching using the standard Internet Protocol (IP).
IPTV Service Provider	Entity that offers IPTV Services and which has a contractual relationship with the Subscriber.
IPTV Solution	The specifications published by the Open IPTV Forum.
IPTV Terminal Function (ITF)	The functionality within the Consumer Network that is responsible for terminating the media and control for an IPTV Service.
Local Storage	Content storage within the administrative realm of the IPTV Service Provider, but not in their physical environment (for example, local storage could be a partition of storage located in the residential network and allocated to the IPTV Service Provider to pre-load CoD).
Network Personal Video Recorder (nPVR)	Provision of PVR functionality whereby the content is stored in the IPTV Service Provider domain. The nPVR allows a user to schedule recording of scheduled content programs. The user can later select the content they want to watch from the recorded content.
Portal	A function of a Service Platform that provides an entry point to individual IPTV Services to Users via a GUI.
Program	A segment of Scheduled Content with a defined beginning and end.
Program Guide	See Content Guide.

Push CoD	A type of Content on Demand where the content is pre-loaded to the ITF local storage by the IPTV Service Provider. The user has no direct control of what content is downloaded; however the IPTV Service Provider may make the choice based on user preferences and habits. Content is available for direct consumption after the user selection is confirmed.
Residential Network	Residential consumer network.
Scheduled Content	An IPTV service where the playout schedule is fixed by an entity other than the User. The content is delivered to the user for immediate consumption.
Service	Content and applications provided by Service Platform Providers and IPTV Service Providers.
Service Access Protection	Means to protect IPTV Services from unauthorized usage/access, such as - Access from unauthorized users - DOS attack
Service Platform Provider	Entity which, based on a contractual relationship with IPTV Service Providers, provides the supporting functions for the delivery of IPTV Services, such as charging, access control and other functions which are not part of the IPTV Service, but required for managing its delivery.
Service Protection	Means to protect contents (files or streams) during its delivery.
Session Portability	Ability of a given service/application to be switched from one device to another for a continuation of a session in real time.
Subscriber	The individual that makes the contract (subscription) with a Service Provider for the consumption of certain services.
Subscription Profile	Information associated with a subscription.
Trick Mode	Facility to allow the User to control the playback of Content, such as pause, fast and slow playback, reverse playback, instant access, replay, forward and reverse skipping.
User Profile	Information (e.g., viewing preferences) associated with a specific User who is a part of a subscription.
User(s)	See End User(s).

3.3 Abbreviations

Abbreviation	***Definition***
ADSL	Asymmetric Digital Subscriber Line
AG	Application Gateway
AKA	Authentication and Key Agreement
AP	Access Point and Authentication Proxy
API	Application Programming Interface
A-RACF	Access Resource Admission Control Function
AS	Application Server
ASM	Authentication and Session Management
AV	Authentication Vector
A/V	Audio and Video
BCG	Broadband Content Guide defined by DVB
BTF	Basic Transport Function
CAC	Connectivity Admission Control
CAS	Conditional Access System
CC	Cluster Controller

CD	Content Delivery
CDC	Connected Device Configuration
CDF	Content Delivery Function
CDN	Content Delivery Network
CDNC	CDN Controller
CE	Consumer Equipment
CG	Content Guide
CK	Ciphering Key
CoD	Content on Demand
CPE	Customer Premise Equipment
CPI	Content Provider Interface
CSP	Content and Service Protection
CSPG	Content and Service Protection Gateway
DAE	Declarative Application Environment
DLNA	Digital Living Network Alliance
DLNA DMS	DLNA Digital Media Server
DLNA DMP	DLNA Digital Media Player
DOS	Denial of Service
DRM	Digital Rights Management
DSCP	DIFFServ Code Point
DTCP-IP	Digital Transmission Content Protection over Internet Protocol
DTT	Digital Terrestrial Television
DVB-IP	Digital Video Broadcasting Internet Protocol
ECMA	European Computer Manufacturers Association, ECMA International - European association for standardizing information and communication systems
EPG	Electronic Program Guide
FE	Functional Entity
GBA	Generic Bootstrapping Architecture
GENA	General Event Notification Architecture
GPON	Gigabit Ethernet Passive Optical Network
GUI	Graphical User Interface
HD	High Definition
HDMI	High Definition Multimedia Interface
HLA	High Level Architecture
HN	Home Network
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IAI	Internet Access Interface
IG	IMS Gateway

IGMP	Internet Group Management Protocol
IMPI	IMS Private User Identity
IMPU	IMS Public User identity
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPTV	Internet Protocol Television
ISIM	IMS Subscriber Identity Module
ISP	Internet Service Provider
ITF	IPTV Terminal Function
M/C-U/C	Multicast to Unicast
LAN	Local Area Network
MAC	Message Authentication Code
MDTF	Multicast Data Terminating Function
MSRP	Message Session Relay Protocol
NAT	Network Address Translation
nPVR	Network Personal Video Recorder
OIF	Open IPTV Forum
OMA	Open Mobile Alliance
OITF	Open IPTV Terminal Function
PAE	Procedural Application Environment
P2P	Peer-to-Peer
PC	Personal Computer
PIM	Protocol Independent Multicast
PLMN	Public Land Mobile Network
POTS	Telephone Service
QoS	Quality of Service
RAC	Resource and Admission Control
RAND	Random Challenge
RCEF	Resource Control Enforcement Function
RTP	Real Time Protocol
RTCP	Real Time Control Protocol
RTSP	Real Time Streaming Protocol
RMS	Remote Management System
RUI	Remote User Interface
SAA	Service Access Authentication
SCART	Syndicat des Constructeurs d'Appareils Radiorécepteurs et Téléviseurs
S-CSCF	Serving Call Session Control Function
SD	Standard Definition

SD&S	DVB Service Discovery and Selection
SDP	Session Description Protocol
SLA	Service Level Agreement
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
SP	Service Provider
SPI	Service Provider Interface
SPDF	Service-based Policy Decision Function
SPP	Service Platform Provider
SSO	Single Sign-on
STB	Set Top Box
TBD	To Be Determined
TCI	Transport and Control Interface
TCP/IP	Transmission Control Protocol/Internet Protocol
UE	User Entity
UI	User Interface
UICC	Universal Integrated Circuit Card
UNI	User Network Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
VoD	Video on Demand
xDSL	Any DSL
WLAN	Wireless LAN
WG	WAN Gateway
WAN	Wide Area Network
XML	eXtensible Markup Language
XHTML	eXtensible Hypertext Markup Language

4. Introduction (Informative)

4.1 IPTV Domains

The Open IPTV Forum recognizes the fact that there are various domains within the end-to-end IPTV value chain that have different administrative control or ownership. Thus, the Open IPTV Forum architecture supports the existence of multiple entities with different regions of administrative control and ownership interests.

Ownership and administrative control are impacted by a variety of factors including the prevailing regulatory regimes, competitive commercial environments, and the commercial strategies of the entities involved. Ownership and administrative control may be considered arbitrary boundaries within certain deployments.

The following domain framework although typical, does not prevent all or some of these domains from being under a single administrative ownership and control.

The architecture recognizes the following domains:

1. Consumer Domain: the domain where the IPTV services are consumed. A consumer domain can consist of a single terminal or a network of terminals and related devices for service consumption. The device may also be a mobile end device; in this case, the delivery system of a network provider is a wireless network. This domain is within the scope for the Open IPTV Forum specifications.

2. Network Provider Domain: the domain connecting customers to platform and service providers. The delivery system is typically composed of access networks and core or backbone networks, using a variety of network technologies. The delivery network is transparent to the IPTV content, although there may be timing and packet loss issues relevant for IPTV content streamed on IP. This domain is within the scope of the Open IPTV Forum specifications.

3. Platform Provider Domain: the domain providing common services (e.g., user authentication, charging etc.) to IPTV Service Providers. Different types of service can be provided to a subscriber including IPTV services, personalized communication services, etc. This domain is within the scope for the Open IPTV Forum specifications.

4. IPTV Service Provider Domain: the domain providing IPTV services to the Consumer Domain. In the context of television services on IP, the IPTV Service Provider acquires/licenses content from Content Providers and packages this into a service. In this sense the IPTV Service Provider is not transparent to the application and content information flow. This domain is within the scope of the Open IPTV Forum specification

5. Content Provider Domain: the domain that owns or is licensed to sell content or content assets. Although the Service Provider is the primary source for the Consumer Domain, a direct logical information flow may be set up between Content Provider and consumer device e.g. for rights management and protection. This domain is within the scope of the Open IPTV Forum specifications, primarily for the aspect of acquisition of content by the service provider. Specifications related to the content development processes of the content provider are NOT considered in scope at this time.

4.2 The IPTV Value Chain

The Open IPTV Forum was established with the intent to specify common and open architectures for supplying a variety of internet multimedia and IPTV services to retail based consumer equipment. The two main services are: Scheduled Content services (the IP equivalent to conventional broadcast TV) and content on-demand content services. Both of those services follow the content value chain shown in Figure 4-1.

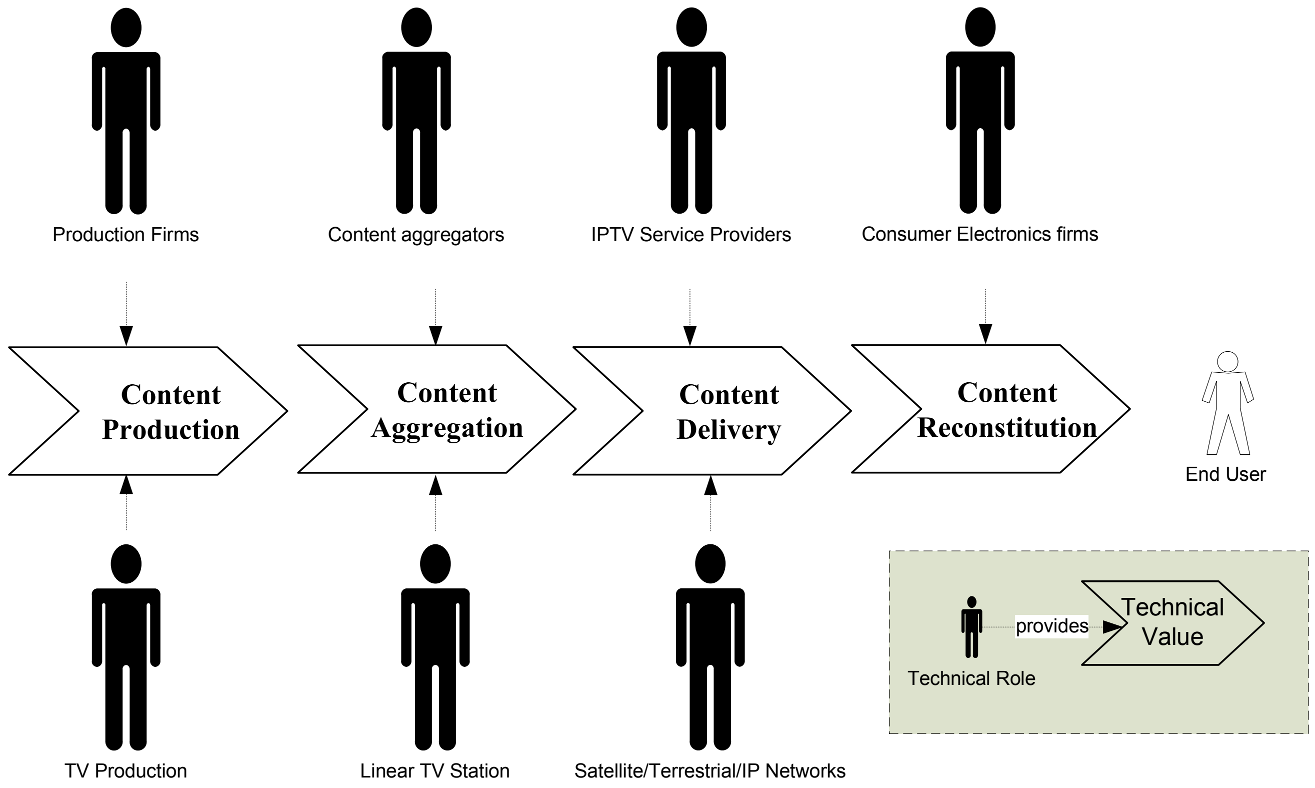


Figure 4-1: Content Value Chain

The content value chain is composed of the following roles to provide Scheduled Content and CoD services:

- Content Production: producing and editing the actual content (movies, drama series, sports events, news reports etc.)
- Content Aggregation: bundling content into catalogue offers and bouquets, ready for delivery
- Content Delivery: transporting the aggregated contents to the consumer
- Content Reconstitution: converting the content into a format suitable for rendering on the end-user device.

Each role in the value chain has historically been bound to a type of stakeholder or technical role. Content Production, for example, is linked to production firms and to the production teams of TV stations.

IPTV technology introduces a set of technical modifications to the content chain that mainly encompasses content aggregation, delivery and reconstitution. The Open IPTV Forum aims at specifying the technology that delivers those three elements in the technical chain. The aforementioned specifications can be distinguished in two main categories:

- **The Managed Model**: concerns access to and delivery of content services delivered over an end-to-end managed network.
- **The Unmanaged Model**: concerns access to and delivery of content services delivered over an unmanaged network (e.g., the Internet) without any quality of service guarantees.

4.2.1 The Managed Model

The managed model deals with content services delivered over an end-to-end managed network. The end user can access content that is made available by the operator. The operator plays the “Content Aggregation” and “Content Delivery” roles:

- Content Provider: provides content and associated metadata to be delivered via the managed operator network. It provides the bundled content to the IPTV service provider through the Content Provider Interface (CPI). A content provider normally retains the rights to the audiovisual content (movies, documentaries, TV programs…etc.). It can be a production company, or a distributor/vendor.

- IPTV Service Provider: is a content aggregator that prepares the content provided by the content provider for delivery by providing additional metadata, content encryption, advertising etc. The Service Provider Interface (SPI) links the IPTV Service Provider to the Service Platform Provider.
- Service Platform Provider: provides the means to control the access to the service prior to delivery to the end user. The Service Platform Provider (SPP) might offer a set of enablers to enrich the IPTV services, such as handling charging information generation. The Transport and Control Interface (TCI) links the Service Platform Provider to the Network Provider
- Network Provider: provides transport resources for delivery of authorized content to the consumer domain. It also provides the communications between the consumer domain and the Service Platform Provider. The User to Network Interface (UNI) links the Network Provider to the consumer domain.

In a typical Managed model, a stakeholder, such as a Telecom Operator, plays the IPTV Service Provider, Service Platform Provider and Network Provider roles, so that high quality services can be guaranteed to the end user.

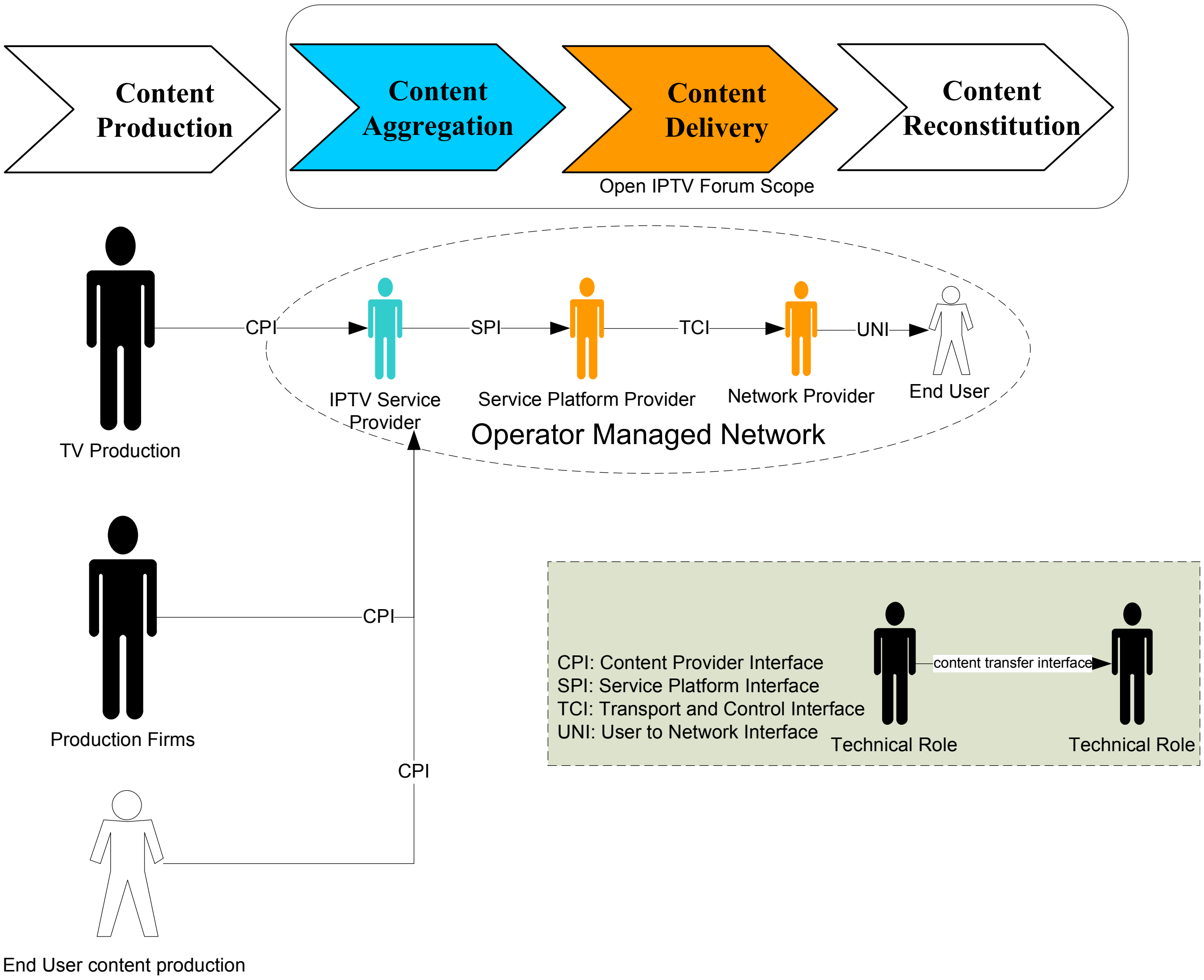


Figure 4-2: Managed Model technical roles and content transfer interfaces

4.2.2 Unmanaged Model

The Unmanaged Model has the same set of technical roles as that of the managed model (See Figure 4-3), but the roles are typically played by different stakeholders. Note that providing services of equivalent quality to those offered by the managed model cannot be easily guaranteed owing to the inherent lack of quality of service guarantees in Internet delivery.

In an Unmanaged Model the relationship between the Service Platform Provider and the Network Provider is not necessarily defined. The role of the Service Platform Provider could be played by an Internet portal.

The Internet Access Interface (IAI) in the Unmanaged Model replaces the TCI in the managed model.

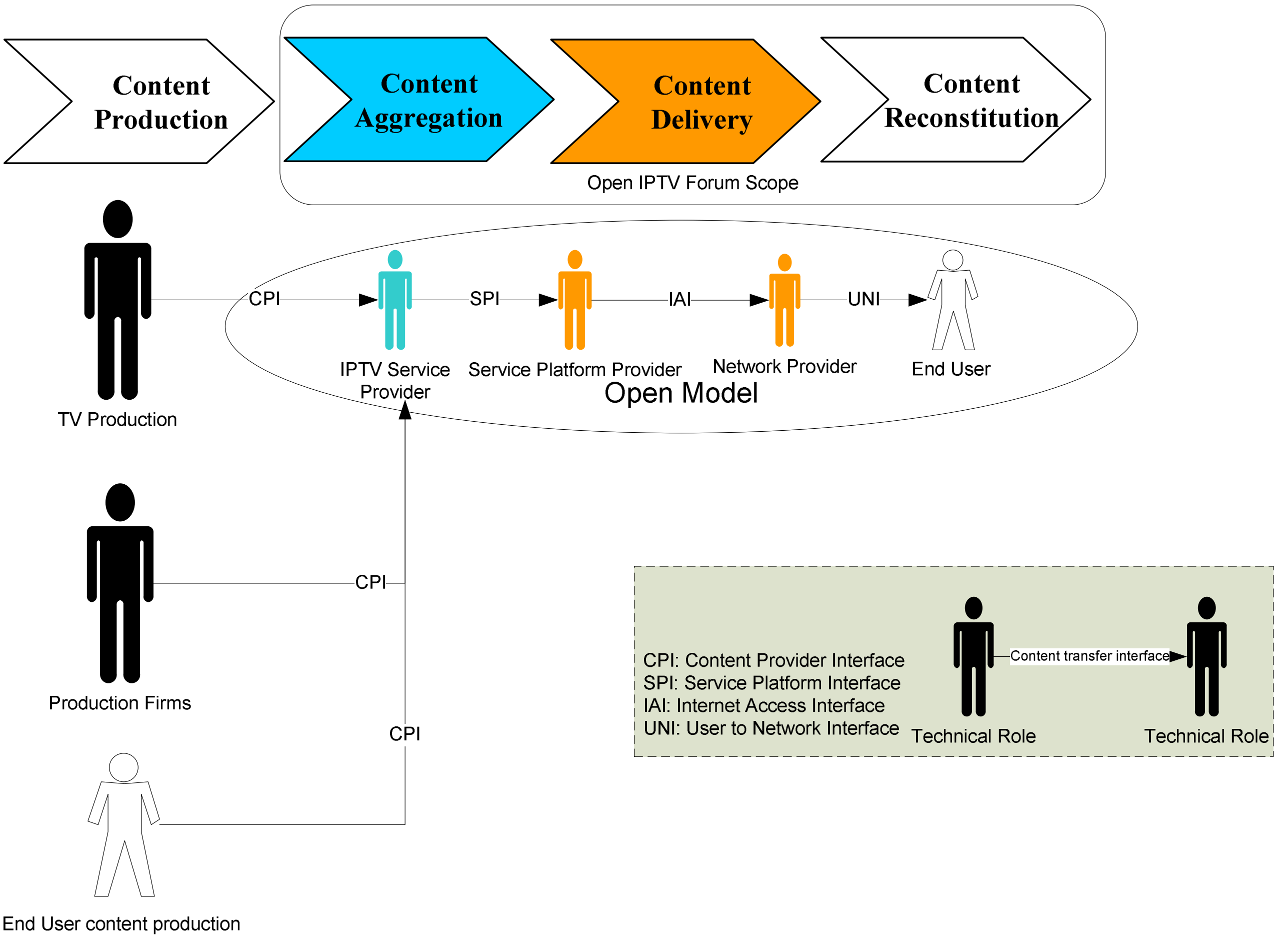


Figure 4-3: Unmanaged Model technical roles and content transfer interfaces

5. High Level Architecture

This section describes the high level architecture for IPTV delivered over both managed and unmanaged networks. To the extent possible, the architecture will be common to both cases. Where this is not the case, the differences will be explicitly highlighted.

The next generation IPTV network must enable services that are distinctly superior to those offered by current IPTV systems. This includes end-user experience, both in terms of user friendliness, as well as personalization, as well as advanced services that adapt to individual usage and lifestyle. Hence, appropriate technologies must be deployed in a flexible architecture that can accommodate new trends and services in a timely fashion.

The high level architecture, described in this section follows a top down approach.

5.1 Reference Points Identification

Figure 5-1 shows the UNI interface between the Consumer Domain and the Network Provider, the Service Platform Provider and the IPTV Service Provider (collectively called “Provider(s) Network”) domains, which is one area of standardization within this specification. Additional interfaces in the network provider domain are also described in this architecture. Future releases of this architecture will provide additional material on interfaces to the content provider and other domains.

The UNI interface is expressed as several sub-interfaces, each of which map to the various functional entities required to provide the necessary support for the end-to-end IPTV service. Reference points are assigned to each of these sub-interfaces. The notation used to identify the sub-interfaces of the UNI, as well as a detailed description for all the reference points, is described later.

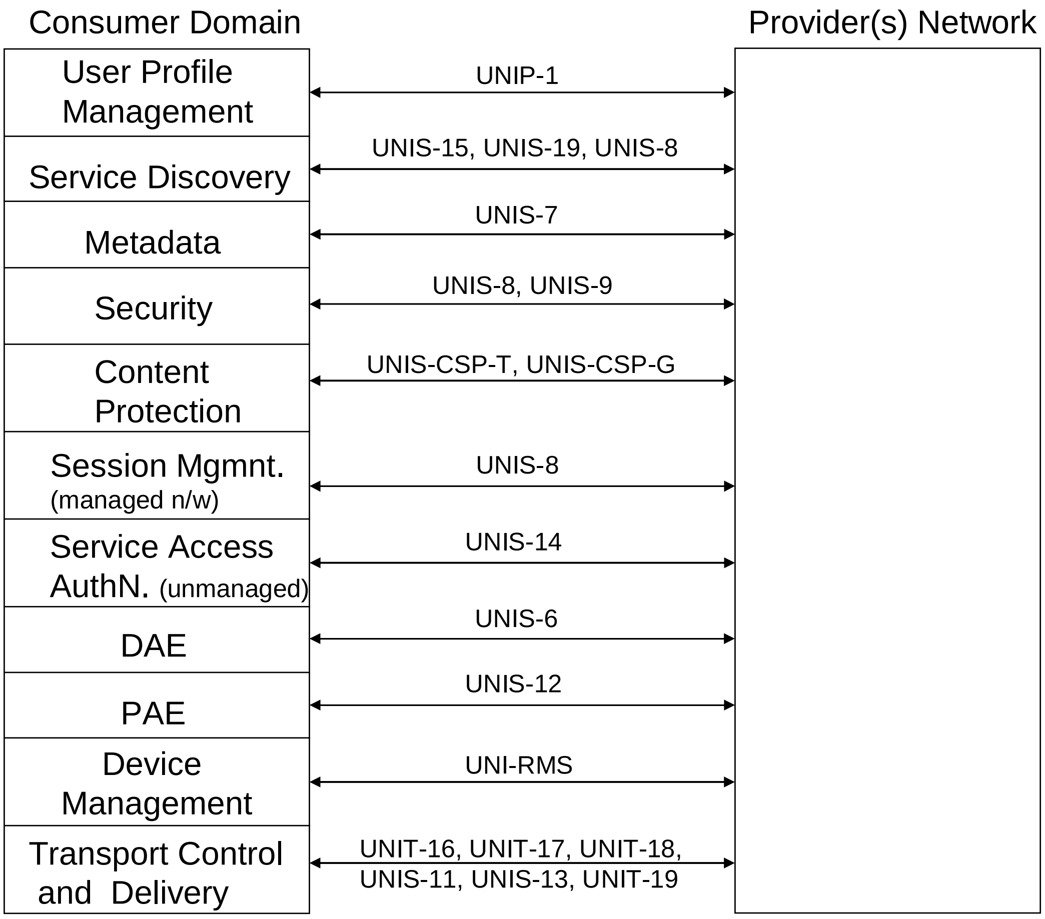


Figure 5-1: Mapping Functional Entities to UNI Reference Points

This mapping is useful to verify compliance of the architecture against the requirements and to be able to document the various functionality supported by the various sub-interfaces in order to fulfil the desired features.

5.2 The Provider(s) Network Architecture

Figure 5-2 depicts the High Level Architecture (HLA) for the Network Provider, the Service Platform Provider and the IPTV Service Provider domains, both for the managed and unmanaged network models.

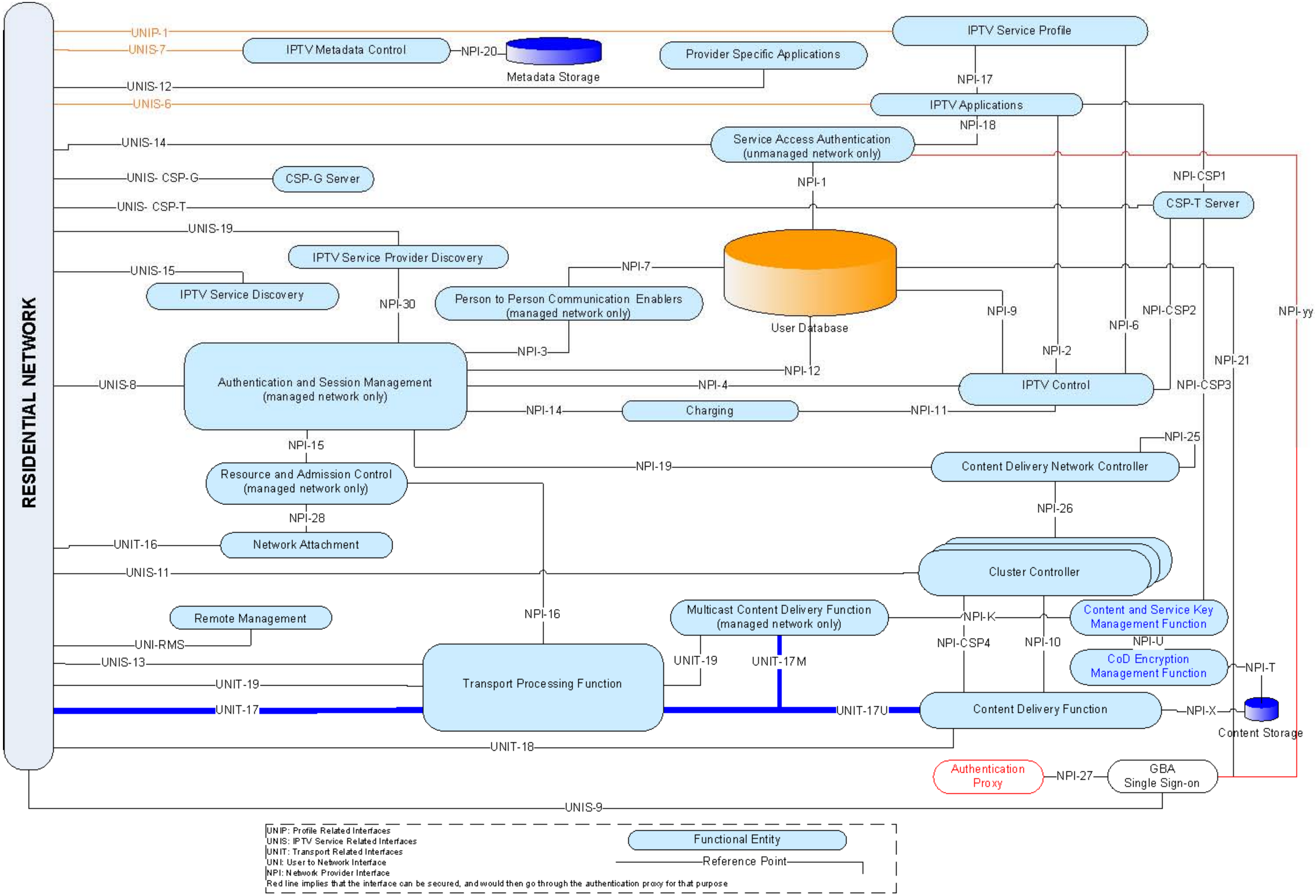

RESIDENTIAL NETWORK
UNIP-1
UNIS-7
IPTV Metadata Control
NPI-20
Metadata Storage
IPTV Service Profile
Provider Specific Applications
UNIS-12
NPI-17
UNIS-6
IPTV Applications
NPI-18
UNIS-14
Service Access Authentication (unmanaged network only)
UNIS- CSP-G
CSP-G Server
NPI-1
NPI-CSP1
UNIS- CSP-T
CSP-T Server
UNIS-19
IPTV Service Provider Discovery
NPI-7
UNIS-15
IPTV Service Discovery
NPI-30
Person to Person Communication Enablers (managed network only)
User Database
NPI-9
NPI-CSP2
NPI-yy
NPI-6
NPI-2
NPI-21
NPI-3
NPI-12
UNIS-8
Authentication and Session Management (managed network only)
NPI-4
IPTV Control
NPI-CSP3
NPI-14
Charging
NPI-11
NPI-15
NPI-25
NPI-19
Content Delivery Network Controller
Resource and Admission Control (managed network only)
NPI-28
NPI-26
UNIT-16
Network Attachment
UNIS-11
Cluster Controller
Remote Management
NPI-16
Multicast Content Delivery Function (managed network only)
NPI-K
Content and Service Key Management Function
UNI-RMS
UNIT-19
UNIT-17M
NPI-CSP4
NPI-10
NPI-U
UNIS-13
CoD Encryption Management Function
NPI-T
UNIT-19
Transport Processing Function
UNIT-17
UNIT-17U
Content Delivery Function
NPI-X
Content Storage
UNIT-18
Authentication Proxy
NPI-27
GBA Single Sign-on
UNIS-9
UNIP: Profile Related Interfaces
UNIS: IPTV Service Related Interfaces
UNIT: Transport Related Interfaces
UNI: User to Network Interface
NPI: Network Provider Interface
Red line implies that the interface can be secured, and would then go through the authentication proxy for that purpose
Functional Entity
Reference Point

Figure 5-2: High Level Architecture for managed and unmanaged networks

The following sections describe the functional elements and reference points depicted in Figure 5-2.

5.2.1 Network Provider Functional Entities

The following is a brief description of the functional entities depicted in Figure 5-2:

Service Access Authentication: This functional entity is responsible for service access protection and authentication of users. The user is identified and authenticated by means of some pre-established credentials (such as user name and password or GBA authentication).

Authentication and Session Management (Managed Network Model only): This functional entity is responsible for the authentication of the user for service access protection, as well as session management for the purpose of coordinating and managing (service accessibility) users' activities and for charging purposes. To this end, the session management ensures that a user request for a service is routed to the appropriate Application Server. This entity has access to the Subscription Profile.

Authentication Proxy (Managed Network Model only): This functional entity establishes a secure communications channel between a network provider's security domain and the ITF. The Authentication Proxy terminates all signalling and control traffic destined to functions within the control of the network provider, and eliminates the need for separate security associations with individual network elements hosting these functions.

GBA Single Sign-on: This functional entity allows Single Sign-on based on the Generic Bootstrapping Architecture. It is used in managed networks, but can also be used in unmanaged networks when a UICC-based IMS authentication is available in the home

IPTV Service Provider Discovery: provides information necessary for the ITF to select IPTV Service Providers, in both the managed and unmanaged models

IPTV Service Discovery: provides information about IPTV services offered by an IPTV service provider, in both the managed and unmanaged models

IPTV Control: This is the main control point for the IPTV solution. It controls the delivery of IPTV services to authorized users. In that regard, it inter-works with the Authentication and Session Management functional entity, which routes incoming/outgoing requests from the IPTV Control to the appropriate destination. This entity has access to the User and Subscription profiles. The IPTV Control generates charging related information.

IPTV Metadata Control: This functional entity performs aggregation of the metadata coming from content providers or third party sources. The IPTV Metadata Control offers basic metadata related to services such as service description, the whole program guide, details related to each event (e.g. description of the film, actors, etc.), program listings and their schedule, personalized Content Guide (CG). This functional entity enables the user to search, discover and initiate immediate viewing or scheduled viewing of future programs and stored content.

IPTV Applications: These include IPTV related services or application logic such as CoD, Push CoD, Content Download, Network PVR, and Messaging as well as Web push/pull service. The function provides end users with IPTV applications using the Declarative Application Environment (DAE).

Provider Specific Applications: This function interacts with the Application Gateway in the consumer domain in order to download generic applications. Provider specific applications run on the AG execution environment. The download can be via push or pull mechanisms. For IPTV, this function can provide end users with provider-specific applications that run in the Procedural Application Environment (PAE) which can manipulate media streams and the Content Guide.

Person-to-Person Communication Enablers (Managed Network Model only): These include interface to various communication services, such as presence, chat, messaging, caller ID notification, etc., for service blending with IPTV related services.

IPTV Service Profile: This functional entity holds the user's profile that is associated with the user's IPTV subscription with an IPTV Service Provider. This profile is consulted by the IPTV Service Provider when the user requests an IPTV service. The profile can be updated by the IPTV Service Provider as well as by an authorized end-user, if allowed by the IPTV Service Provider.

User Database: The central database of Subscription profiles, managed by the Service Platform Provider. The nature of this may vary between managed and unmanaged systems, and would typically includes data that is not IPTV service specific such as authentication information, communication related information, etc.

The Content Delivery Network (CDN): This is a fundamental functionality in an IPTV CoD solution, since it allows the optimization of the network use through a distribution of the media servers in the physical network, and the optimization of the storage resources through a popularity-based distribution of the content on the media servers. This results in having popular content massively distributed on media servers at the edge of the network (as close as possible to the customer) while less popular content are distributed on a reduced number of media servers. The Content Delivery Network contains three intelligent sub functions:

- **Content Delivery Network Controller (CDNC):** This functional entity performs cluster[1] selection in the CDN, based on the request issued by the IPTV Control functional entity. Many instances of a CDN controller may coexist in the same CDN. They may interact for the purpose of selecting the right cluster.
- **Cluster Controller (CC):** This functional entity manages a set of Content Delivery Functions (a cluster of CDFs).
  - It terminates IPTV service session setup
  - It handles content delivery session setup
  - It proxies all message exchanges between CDFs and the ITF.
  - It maintains the state of the media servers (Content Delivery Functions)
- **Content Delivery Function (CDF):** This functional entity is responsible for media processing, delivery and distribution, under the control of the Cluster Controller.

Multicast Content Delivery Function: This entity is responsible for delivery of content and generic data to the OITF by means of multicast, using multicast streams and the multicast data channel respectively. In the content streaming case, this is the so-called head end. In the data case it is the source of the multicast data channel.

Network Attachment: This functional entity includes the functions associated with provisioning of IP addresses, network level user authentication and access network configuration. For the unmanaged model, this function is provided by the user’s access network provider.

Transport Processing Function: This functional entity includes the functions needed to support real-time multicast and unicast streams, optimizing network usage in the physical network, and enforcing related traffic policies coming from Resource and Admission Control.

Resource and Admission Control (Managed Network Model only): In a managed network, Resource and Admission Control provides policy control and resource reservation for the required transport resources, for both unicast and multicast delivery. In this capacity, it interacts with the authentication and session management functional entity and the Transport processing function.

Charging: This functional entity includes the charging mechanisms at the platform level available to all the IPTV Service Providers, for all the users managed by the Service Platform Provider. The charging subsystem collects network and platform related events that can be later used for billing and statistical analysis purposes. The IPTV service providers are free to build their own billing systems that could be based on common charging but also be completely independent (e.g. based on the CSP and CAS). The IPTV service provider’s billing mechanisms are out of the scope of this specification.

CSP-T Server: This functional entity handles service protection and content protection for the CSP-T client in the OITF. It is used to enable the key management necessary to implement service protection and content protection.

[1] The term Cluster corresponds to a logical association of one or more "Content Delivery Functions" which share some resources (such as location, storage capacity etc.).

CSP-G Server: This functional entity handles service protection and content protection for the Content and Service Protection Gateway (CSPG) in the residential network. The solution for service and content protection is specific to the IPTV service provider. Therefore, network reference points are not specified by this specification and interfaces are defined by the IPTV Service Provider.

Remote Management: In a managed network, this entity provides the server-side functionalities to remotely manage the residential network devices, for both provisioning and assurance purposes: the functions provided relates to configuration management (including firmware upgrade), fault management (including troubleshooting and diagnostics), and performance monitoring.

Content and Service Key Management Function: Entity responsible for storing and providing Service, Program, Content Keys and ECM attached information. This function may be physically co-located with other functions, (e.g. the Content Delivery Network Controller for Content on Demand services.) This entity has been identified in release 1 just to illustrate informatively the separation between content encryption, which is part of content preparation, and content delivery.

Content on Demand Encryption Management Function: Back office Content on Demand function in charge of launching Content on Demand encryption using a Content Key. This entity has been identified in release 1 just to illustrate informatively the separation between content encryption, which is part of content preparation, and content delivery.

5.2.2 Mapping between HLA and IPTV Domains (Informative)

Table 1 provides an informative mapping between the functional entities depicted in the HLA and the IPTV domains as defined in Section 4.1.

Functional Entity	**Domain assignment**
Network Attachment	Network Provider
Authentication and Session Management (Managed Network Model only)	Service Platform Provider
User Database	Service Platform Provider
IPTV Control	Service Platform Provider
Person to Person Communication Enablers (Managed Network Model only)	Service Platform Provider
IPTV Applications	IPTV Service Provider
Content Delivery Network Controller	Network, Platform and IPTV Service Providers
Content Delivery	Network, Platform and IPTV Service Providers
IPTV Metadata Control	IPTV Service Provider
IPTV Service Discovery	Service Platform Provider, IPTV Service Provider
IPTV Service Provider Discovery	Service Platform Provider
IPTV Service Profile	IPTV Service Provider
Provider Specific Applications	IPTV Service Provider
Multicast Content Delivery Function	Network, Platform and IPTV Service Providers
Metadata Storage	IPTV Service Provider

Service Access Authentication (Unmanaged Network Model only)	Service Platform Provider
Charging	Service Platform Provider
Cluster Controller	Network, Platform and IPTV Service Providers
Resource and Admission Control (Managed Network Model only)	Network Provider
Transport Processing Function	Network Provider
Authentication Proxy (Managed Network Model only)	Service Platform Provider
GBA Single Sign-on	Service Platform Provider
CSP-T Server	IPTV Service Provider
CSP-G Server	IPTV Service Provider
Content and Service Key Management Function	IPTV Service Provider
Content on Demand Encryption Management Function	IPTV Service Provider
RMS	Network Provider, Service Platform Providers

Table 1: Functional Entity domain assignment

5.2.3 Reference Points Description

5.2.3.1 UNI Reference Points

The UNI is expressed as several reference points, each of which map to the various functional entities required to provide the necessary support for the end-to-end IPTV service. The notation used to identify the reference points of the UNI, as well as a detailed description for all the reference points, is described later.

Reference Point	***Description***
UNIP-1	Reference point for user initiated IPTV service profile management
UNIS-6	Reference point for user interaction with application logic for transfer of user requests and interactive feedback of user responses (provider specific GUI). HTTP is used to interface between the DAE and the IPTV Application Function in both the managed and unmanaged models**.**
UNIS-7	Requests for transport and encoding of content guide metadata. The reference point includes the metadata and the protocols used to deliver the metadata, and shall be based on DVB-IP BCG. [Ref 13]
UNIS-8	Authentication and session management for the managed network model.
UNIS-9	Authentication for GBA Single Sign-on
UNIS-11	Reference point for control of real time streaming (e.g. control for pause, rewind, skip forward). This reference point is optionally secured. The reference point includes content delivery session setup in case of the unmanaged model.
UNIS-12	Reference point between the AG (see section 5.3.1.3 for details) and the provider specific application functional entity. Encompasses two functions: • Signalling and download of applications in a generic format. (Subject to standardization) • Interaction of generic applications with the provider network. (Not subject to standardization)

UNIS-13	User Stream control for multicast of real time content and data for the managed network model. The protocol used on this interface is IGMP. [Ref 10]
UNIS-14	Reference point used for authorization of service access for the managed and unmanaged network models.
UNIS-15	Reference point to the IPTV Service Discovery FE to obtain information about IPTV services offered by an IPTV Service Provider
UNIT-16	Network attachment functions connected to this reference point include: DHCP Server and Relay.
UNIT-17	Content stream including content; content encryption (for protected services) and content encoding. This reference point can be used for both multicast and unicast (UNIT-17M and UNIT-17U, respectively). This could be RTP and HTTP (unicast only).
UNIT-18	Performance monitoring interface for reporting the performance monitoring results. A possible protocol is RTCP.
UNIT-19	Multicast Data Channel. Used to deliver data of different kinds to the OITF by means of multicast. This reference point can carry discrete data that is carried over unicast through e.g. the interfaces UNIS-6, and UNIS-7. Other uses e.g. UNI-RMS are not excluded.
UNIS-19	Reference point to the IPTV Service Provider Discovery functional entity to obtain the list of Service Providers, and related information.
UNI-RMS	Remote Management of end user devices (based on the DSL Forum TR-069 [Ref 1] framework and related extensions based on DVB-IP-RMS specification)
UNIS-CSP-T	Rights management for protected content – including key management and rights expression.
UNIS-CSP-G	Reference point to support a service and content protection solution which is specific to IPTV Service Provider. This interface may be used to obtain licenses for purchased/subscribed content, control content and service protection system and also deliver content.

Table 2: UNI Reference Points

5.2.3.2 Network Reference Points Description

Reference Point	***Description***
NPI-1	Reference point between the Service Access Authentication FE and the User Database.
NPI-2	An optional reference point allowing interaction between IPTV Applications and the IPTV Control FE. This is not subject to standardization.
NPI-3	The reference point between Authentication Session Management and Person-to-Person Communication Enablers. (This is the ISC interface defined by 3GPP) [Ref 15]
NPI-4	Reference point for routing of IPTV service related messages to the IPTV Control Point. This is the ISC reference point defined by 3GPP [Ref 15].
NPI-6	This reference point allows the IPTV Control Point to retrieve the subscriber’s IPTV-related service data when a user registers in the IMS network. (Not subject to standardization)
NPI-7	This reference point allows Person-to-Person Application Enablers to retrieve the subscriber’s IMS data from the User Database. This is the Sh interface defined by 3GPP [Ref 15].
NPI-9	This reference point allows the IPTV Control Point to retrieve the subscriber’s IMS-specific data from the User Database. This is the Sh interface defined by 3GPP. [Ref 15]
NPI-10	An optional reference point for the allocation/de-allocation and control of content for a specific unicast session.

NPI-11	A reference point for sending events and charging information. This is the Rf reference point defined by 3GPP [Ref 15].
NPI-12	This reference point allows the Authentication and Session Management FE to retrieve the subscriber's IMS data from the User Database as a part of the user's IMS registration. This is the Cx interface defined by 3GPP [Ref 15].
NPI-14	Same as NPI-11
NPI-15	This reference point controls the Resources and Admission Control. It is the Gq' interface defined by ETSI TISPAN. [Ref 15]
NPI-16	Reference point between the Transport Processing Function and Resource and Admission Control. It is the Re interface (Diameter based) [Ref 15]
NPI-17	Reference point between the IPTV Applications and the IPTV Service Profile.
NPI-18	Reference point between the Service Access and Authentication FE and the IPTV Applications. This is only used in the unmanaged network model
NPI-19	This reference point is used for unicast session control between the Authentication and Session Management and the Content Delivery Network Controller
NPI-20	This optional reference point allows the retrieval of CG data. (Not subject to standardization)
NPI-21	This reference point allows the GBA Single Sign-on functional entity to validate user credentials
NPI-25	This reference point allows proxying unicast control messages to locate the appropriate Content Delivery Network Controller FE.
NPI-26	The reference point allows the Content Delivery Network Controller to delegate the handling of a unicast session to a specific Cluster Controller.
NPI-27	The reference point between the Authentication Proxy and the GBA Single Sign-on node allows the proxy to retrieve a user key for authentication purposes.
NPI-28	This reference point is used to push the user access capabilities to the Network Attachment and the RAC. This is the e4 interface defined by 3GPP [Ref 15].
NPI-30	This reference point supports the IPTV Service Provider Discovery step of the service discovery procedure for managed model. This is the ISC interface defined by 3GPP [Ref 15].
NPI-CSP-1	Reference point to confirm whether a Marlin content license can be issued for the request received via UNIS-CSP-T. This interface is not specified by this version of the specification.
NPI-CSP1a	Reference point used by the Marlin DRM system to include business information or a reference to business information into a DRM request (e.g. license request) as requested via UNIS-CSP-T, and the subsequent confirmation and retrieval of this business information when the DRM request is consumed. This interface is not specified by this version of the specification.
NPI-CSP-2	Reference point, used in the managed network model, to retrieve information on the appropriate cluster controller in the Content Delivery Network that will serve a particular request for purchased or subscribed-to content. This chosen cluster controller will be contacted by the CSP-T Server functional entity via NPI-CSP3. This interface is not specified by this version of the specification.
NPI-CSP-3	Reference point to retrieve the appropriate encryption key needed to prepare a Marlin content license for the chosen content. It is the content encryption key for downloadable content or the key that encodes the Marlin short term key message that contains the key that encodes the streaming media. This interface is not specified by this version of the specification.

NPI-CSP-4	Reference point to provide content encryption keys to the content delivery function for encrypting the downloadable content or for requesting/generating the Marlin short term key messages that accompany the encoded streaming media. This interface is not defined by this version of the specification.
NPI-yy	Reference point that provides GBA authentication mechanism to the Service Access Authentication Function.
NPI-T	Reference point where the encrypted content is stored on the content storage entity for delivery by the Content Delivery Function. This interface is not specified by this version of the specification. This interface has been identified in release 1 just to illustrate informatively the separation between content encryption, which is part of content preparation, and content delivery.
NPI-U	Reference point where the content Service, Program and Content Keys and ECM attached information are provided to the Content Management Function. This interface is not specified by this version of the specification. This interface has been identified in release 1 just to illustrate informatively the separation between content encryption, which is part of content preparation, and content delivery.
NPI-K	Reference point where the content Service, Program and Content Keys and ECM attached information are provided to the Multicast Content Delivery Function for multicast stream Encryption. This interface is not specified by this version of the specification. This interface has been identified in release 1 just to illustrate informatively the separation between content encryption which is part of content preparation and content delivery.
NPI-X	Reference point where the On Demand Content is fetched by the Content Delivery Function for delivery. This interface is not specified by this version of the specification. This interface has been identified in release 1 just to illustrate informatively the separation between content encryption, which is part of content preparation, and content delivery.

Table 3: Network Reference Points

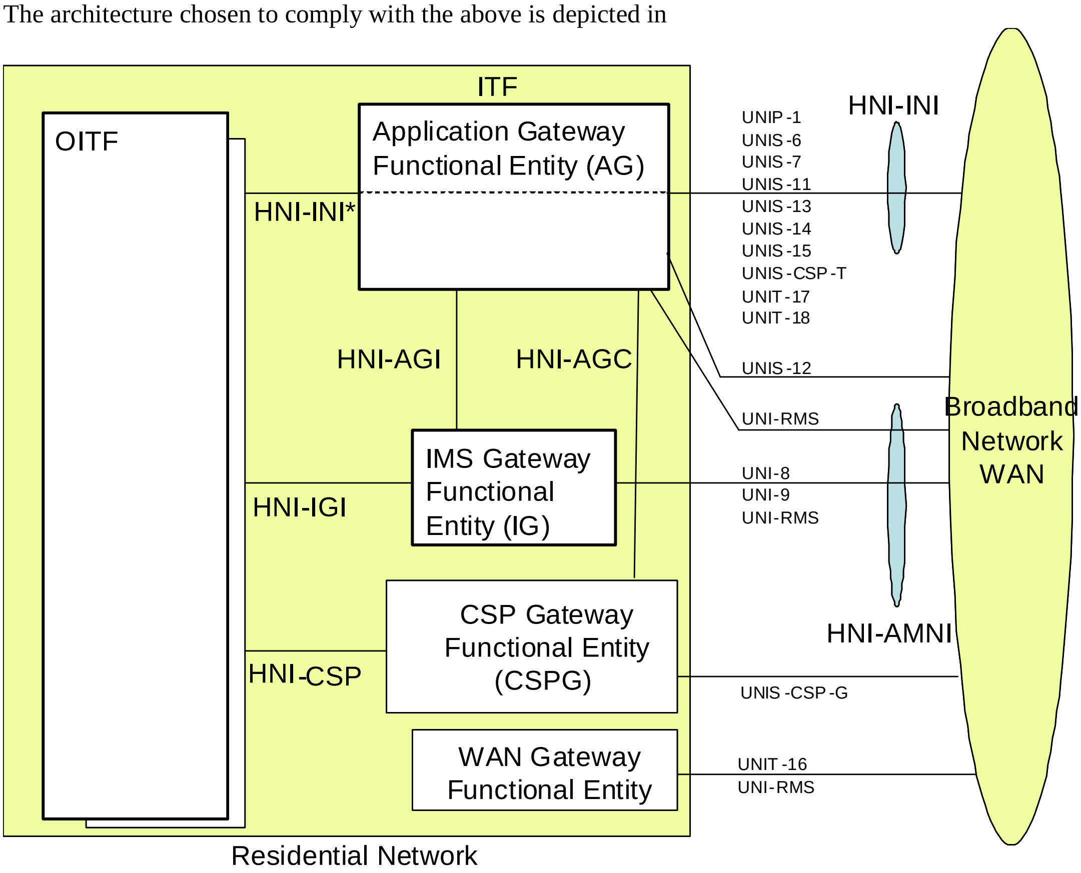
5.3 Residential Network High-Level Architectural Overview

The architecture of the consumer domain (referred to hereafter as the residential network) is as shown in Figure 5-3: Residential Network Architecturesand composed of 5 functional entities, with well defined interfaces between them, and where each functional entity includes a number of functions. As shown in Figure 5-3, the entire collection of these functional entities is called the IPTV Terminal Function (ITF).

The residential network architecture is designed to:

- Support multiple deployment scenarios.
- Allow non-IPTV applications to co-exist with IPTV services, but be able to execute independently from the IPTV service.

The architecture chosen to comply with the above is depicted in Figure 5-3 below.



There are two main interface groups between the Residential Network and the Provider(s) Network domain: the HNI-INI and the HNI-AMNI. The mapping between these key functional groupings and UNI reference points is depicted in the

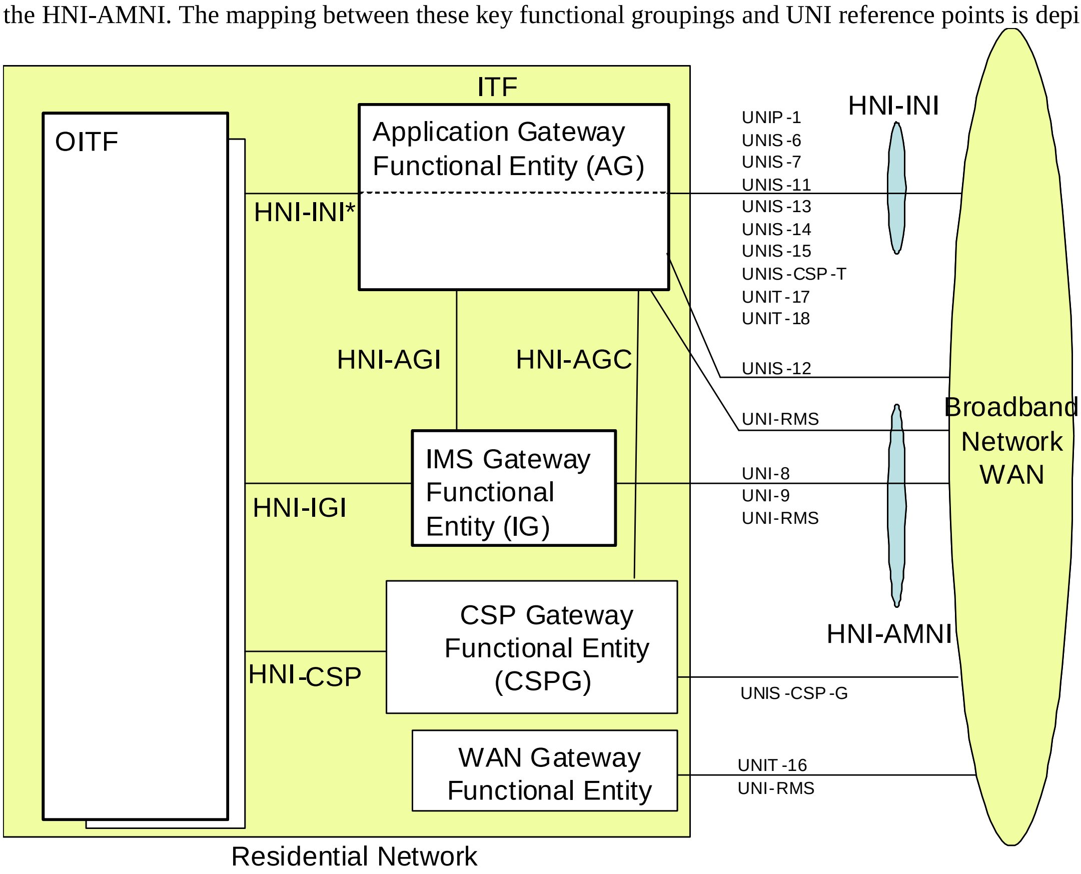


Figure 5-3.

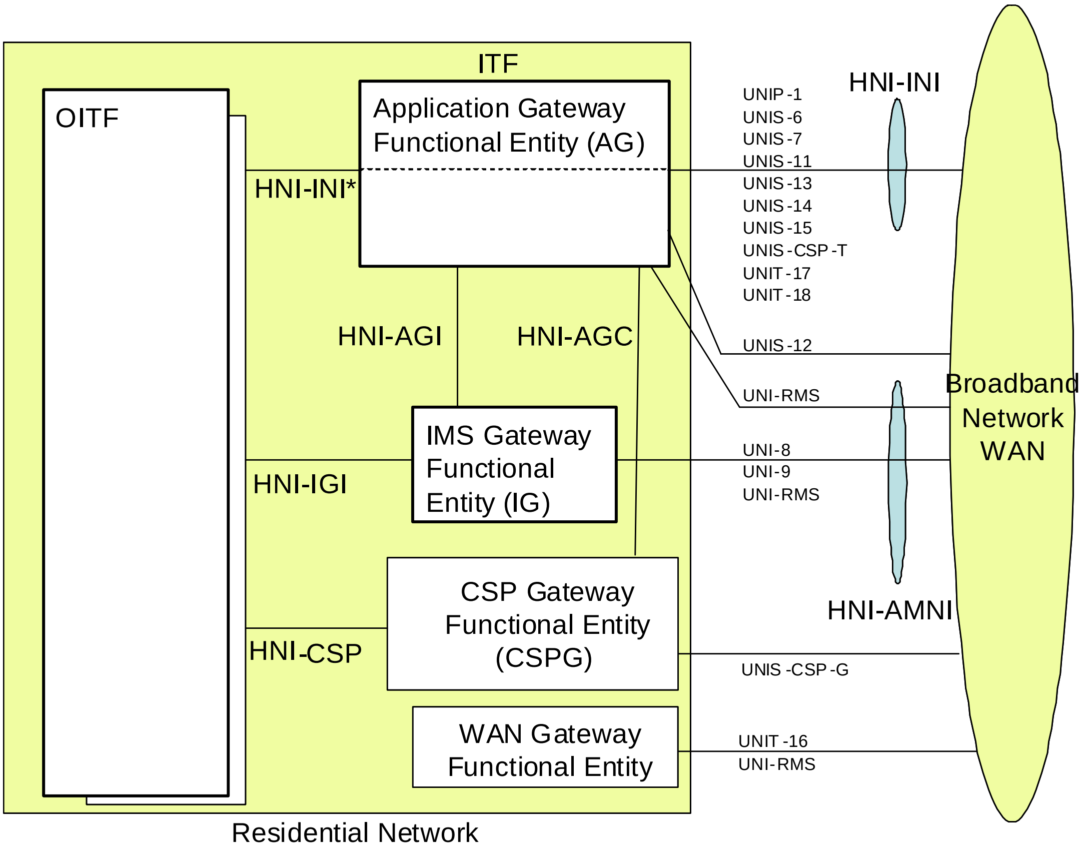


Figure 5-3: Residential Network Architectures

Below is a brief description of the functional entities in the residential network:

1) Open IPTV Terminal Functional Entity (OITF)

The OITF includes the functionality required to access IPTV service for both the unmanaged and the managed network models through the HNI-INI and HNI-IGI interfaces.

- To access the IPTV services using the unmanaged model, the OITF only needs to use the HNI-INI interface. Thus, the minimum set of functional entities needed to access unmanaged IPTV services are the OITF and the WAN Gateway.
- To access IPTV service using the managed network model, the OITF needs to use both the HNI-INI and the HNI-IGI interfaces. Thus, the minimum set of functional entities needed to access the managed IPTV services are the OITF, the IG and the WAN Gateway (as it provides the physical connection between the residential network and the WAN). The HNI-IGI interface requires special protection, as it carries credentials/secrets.

The OITF has its own direct user interaction (e.g., remote control, keyboard) and audio/video rendering and, optionally, grabbing functionalities (e.g. display, speakers, cameras, microphones) or can be directly connected with other audio/video rendering/grabbing devices without passing through home network communication.

All Residential Network deployments will have at least one instance of the OITF.

The OITF may include functions to allow Open IPTV Forum defined services to be accessed on DLNA devices [Ref 2].

2) IMS Gateway Functional Entity (IG)

The IG includes the necessary functionality to allow an OITF device to access managed network services, based on an IMS core network, through the HNI-IGI interface. The IG provides an IPTV end user with access to managed network IPTV services and to blended person-to-person communication services such as Chat, Messaging, Presence, etc. Support for unsolicited notification is also included for such services as Presence, Caller ID, etc.

The IG is able to offer its functionality to the AG via the HNI-AGI interface.

Support for new or enhanced applications can be realized by a firmware upgrade to the IG without any impacts on the OITF functionality.

3) Application Gateway Functional Entity (AG)

The Application Gateway (AG) is an optional gateway function that incorporates a procedural language based application execution environment where applications can be remotely downloaded for execution. This functionality is required by certain service providers that wish to have generic procedural language based applications related or unrelated to IPTV services downloaded for execution in the home environment. Examples of applications related to IPTV services include an EPG generating a remote UI; proxying for signalling protocols when not involving SIP, and when client and server are not in same IP domain; support for proprietary or non-standard content download protocols (where the AG has A/V content storage capability); insertion of personalized advertisements in media stream; and full blended person-to-person communication services (e.g., videoconference using a TV set as a display). An example of an application unrelated to IPTV services is one that collects alarms from home devices.

To interface to the AG, an OITF uses the HNI-INI* interface. The HNI-INI* is a selection from the reference points in the HNI-INI interface in addition to support for discovery of an AG by an OITF.

When present, the AG, through application running in the executable application environment, can perform any of the following functionalities:

- Manipulate media streams.
  Note that for protected content, this is only addressed when the AG and the CSPG are combined in the same device and that the Release 1 specification does not define the routing of media content (for the purposes of media control) via an AG which is not also a CSPG.

- Filter Content Guide (CG) data; insert its own CG data.
  Note that for the Release 1 specifications, this is only addressed where the resulting content guide is output from the AG to the OITF in the form of a remote UI. The Release 1 specifications do not define how an AG may output CG data in BCG format to an OITF or how an OITF may discover that BCG format information is available from an AG.

- Support proprietary applications through a Remote User Interface (RUI).

- Support for proprietary or non-standard content download protocols

- Support advanced blended communication services.

When the AG is deployed in a device with local graphics rendering (e.g. combined with an OITF), applications running in the PAE can offer a wide range of applications and services directly using that local graphics rendering system without using a remote UI.

The AG is able to make use of the services of the IG via the HNI-AGI interface. This interface is not defined in the Release 1 specifications; however, where an AG and an OITF are combined in the same device, the device may use the HNI-IGI interface for both DAE and PAE applications.

4) Content and Service Protection (CSP) Gateway Functional Entity (CSPG)

The CSP Gateway (CSPG) is an optional gateway functional entity that provides a conversion from a content and service protection solution in the network to a secure authenticated channel between the CSPG and the OITF.

5) WAN Gateway Functional Entity (WG)

The WAN Gateway function supports the physical connection between the residential LAN and the Access Network WAN. A WAN gateway functional entity will exist in all deployments although not all its functions will be required in all cases.

5.3.1 Residential Network Functional Entities

The following is a more detailed description of the various functional entities identified above.

For ease of understanding of the detailed functional description of the residential network, this specification uses a stepwise build up of the residential network functional entities comprising of the following steps:

- OITF and WAN Gateway (WG)
- OITF, WG and IG
- OITF, WG, IG and the optional functional entities AG and CSPG

Note that this build-up of functions does not imply that these combinations of functions are the only deployment options possible. Each of OITF, IG, AG, CSPG and WAN Gateway functional entities may be deployed as separate physical devices in the residential network or in combinations or may not be deployed at all in the case of the optional entities AG and CSPG as described in Section 5.3.4.

5.3.1.1 Open IPTV Terminal Functional Entity (OITF)

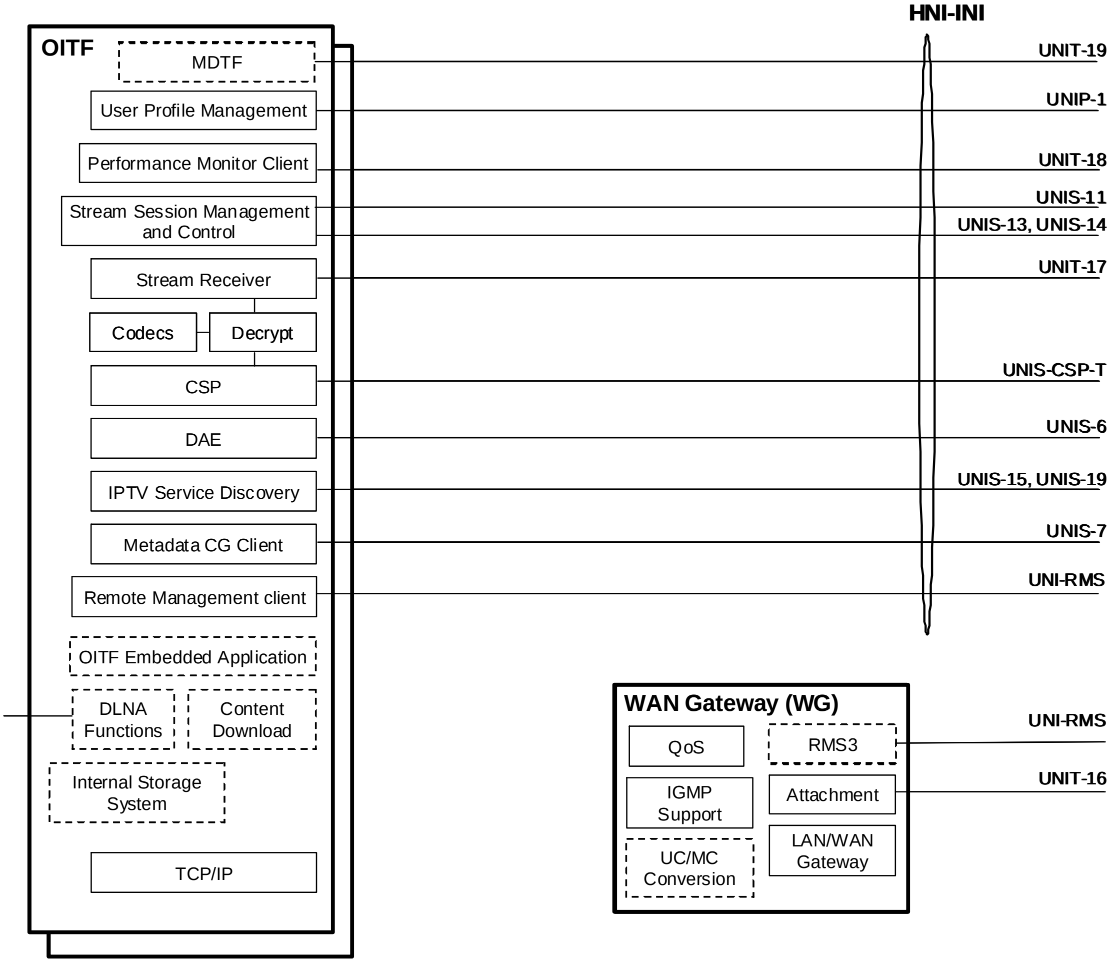


Figure 5-4: OITF functions and interfaces exposed

The **OITF** functional entity shown in Figure 5-4 includes the following functions:

User Profile Management: Manages subscription information associated with a specific User, e.g., viewing preferences. The user profile management functions include the ability to create, fetch, modify, delete, replace user profiles.

Stream Session Management and Control: Initiates and terminates content delivery sessions. Manages content delivery sessions, including trick play control of unicast streams and multicast stream control. It applies to both the unmanaged and the managed models.

Stream Receiver: Receives streamed content from the network and includes stream buffering in the case of progressive download. The function applies to both the managed and unmanaged models, although different technologies might be chosen for each case.

Codecs: A/V codecs for all streamed and downloaded content. It includes decoding, scaling and rendering functions.

CSP: Client side key management for the terminal centric approach to service protection and content protection. Enforces content usage rules in the client. It applies to both the managed and the unmanaged models. See CSP Gateway Functional Entity for the alternative gateway centric approach to service and content protection.

Content Download: Reception of content downloaded to the client in non-real time. Content download might be unicast or multicast. For multicast, the MDTF is used. Local storage is required for content download. It applies to both the managed and the unmanaged models. This function is optional.

MDTF (Multicast Data Terminating Function): This function receives generic data sent over multicast. Content types that can be distributed to MDTF include Content Guide data, static DAE content, video content, interactivity information, notifications, software releases and patches.

Decrypt: Removes any encryption applied to the content, under the control of the CSP function. This function is not used for unencrypted content. It applies to both the managed and the unmanaged models.

Declarative Application Environment (DAE): A declarative language based environment (browser) based on CEA-2014 [Ref 3] for presentation of user interface and including scripting support for interaction with network server-side applications and access to the APIs of the other OITF functions.

The specification of the DAE declarative language environment including the APIs available to the downloaded applications is within the scope of the Forum.

The DAE can also query, internally to the OITF, the Metadata-based Content Guide Client in order to extract any data it may contain.

The downloaded applications that run in the DAE are considered to be Service Provider specific and therefore will not be defined by the Forum's specifications.

Metadata-based Content Guide Client: Client for metadata-based content guides. The user interface including the presentation of metadata-based content guide is OITF vendor dependent and is out of scope of this specification. This function may also make the metadata available to Residential Network devices via the DLNA Functions function. It applies to both the managed and the unmanaged models.

Remote Management Client: provides the client-side functions to remotely manage the OITF, for both provisioning and assurance purposes. The functions provided relate to configuration management (including firmware upgrade) and fault management (including troubleshooting and diagnostics). When realized as standard TR-069 client, it uses the UNI-RMS interface (providing also performance monitoring); otherwise, remote management is supported as a DAE application which uses the UNIS-6 interface.

IPTV Service Discovery: Function for discovering IPTV Service Providers and related services. It applies to both the unmanaged and the managed models. Note that different aspects of DVB SD&S [Ref 4] may apply to the different models.

Integral Storage System: Storage for content download and PVR based functions. This function is optional but will be required if Content Download is supported.

DLNA Functions: Implements DLNA DMS [Ref 2] functions to expose and distribute content in a DLNA compliant manner through the residential network. The DLNA Functions function may also offer a DLNA DMP [Ref 3] function to locate and select content available from other DMS in the residential network. The selected content can be streamed across the residential network and rendered by the OITF. This function is optional.

OITF embedded application: This optional function provides embedded applications for IPTV services, e.g. local PVR, using the standardized interfaces which are defined as UNI and HNI-IGI. The user interaction with this function is OITF vendor specific

Performance Monitor Client: Client for providing feedback on service quality – for example, pixilation, frame loss, packet loss and delay (the exact information to be provided is to be specified other specifications). It applies to both the managed and the unmanaged models.

The **WAN Gateway** Functional Entity shown in Figure 5-4 contains the following functions:

LAN/WAN Gateway: Supports the physical termination of the access network (e.g. xDSL, GPON etc.) and the layer 2, layer 3 and higher services (such as NAT, IGMP proxy-routing) required to support IPTV and other services terminated in the residential network that share the WAN connection.

Attachment: Attachment function is responsible for the attachment of the residential network to the Network Provider.

RMS3: Depending on the provider model, the WAN Gateway may be remotely monitored and configured by the access service provider. The RMS function supports the interface to the remote manager (i.e. TR-069 CWMP remote management protocol [Ref 1], plus TR-098 device data model [Ref 33] with possible extensions.)

QoS: The QoS function provides classification, marking, re-marking, policing, and queuing of Ethernet and IP traffic that goes between the WAN and LAN interfaces. Marking and re-marking of Ethernet priority and Diffserv code points (DSCP) [Ref 6] is supported. Classification can occur through a variety of characteristics of IP traffic, including Ethernet priority, DSCP, origination and destination IP address, and application protocol.

IGMP Support: Provides the functions for IGMP Proxy and IGMP Snooping. The IGMP Proxy allows multiple in-home devices in the residential network to be able to join the same multicast stream. IGMP Snooping is the process of listening to IGMP traffic to allow, when present, the switch to "listen in" on the IGMP conversation between hosts and routers by processing the layer 3 IGMP packets sent in a multicast network to avoid flooding (see 5.3.3.1).

UN/MC Conv: The WAN Gateway may have this function to avoid some problems due to the low efficiency and unreliability of multicast on wireless networks. This function is not specified in Release 1.

5.3.1.2 OITF and IG

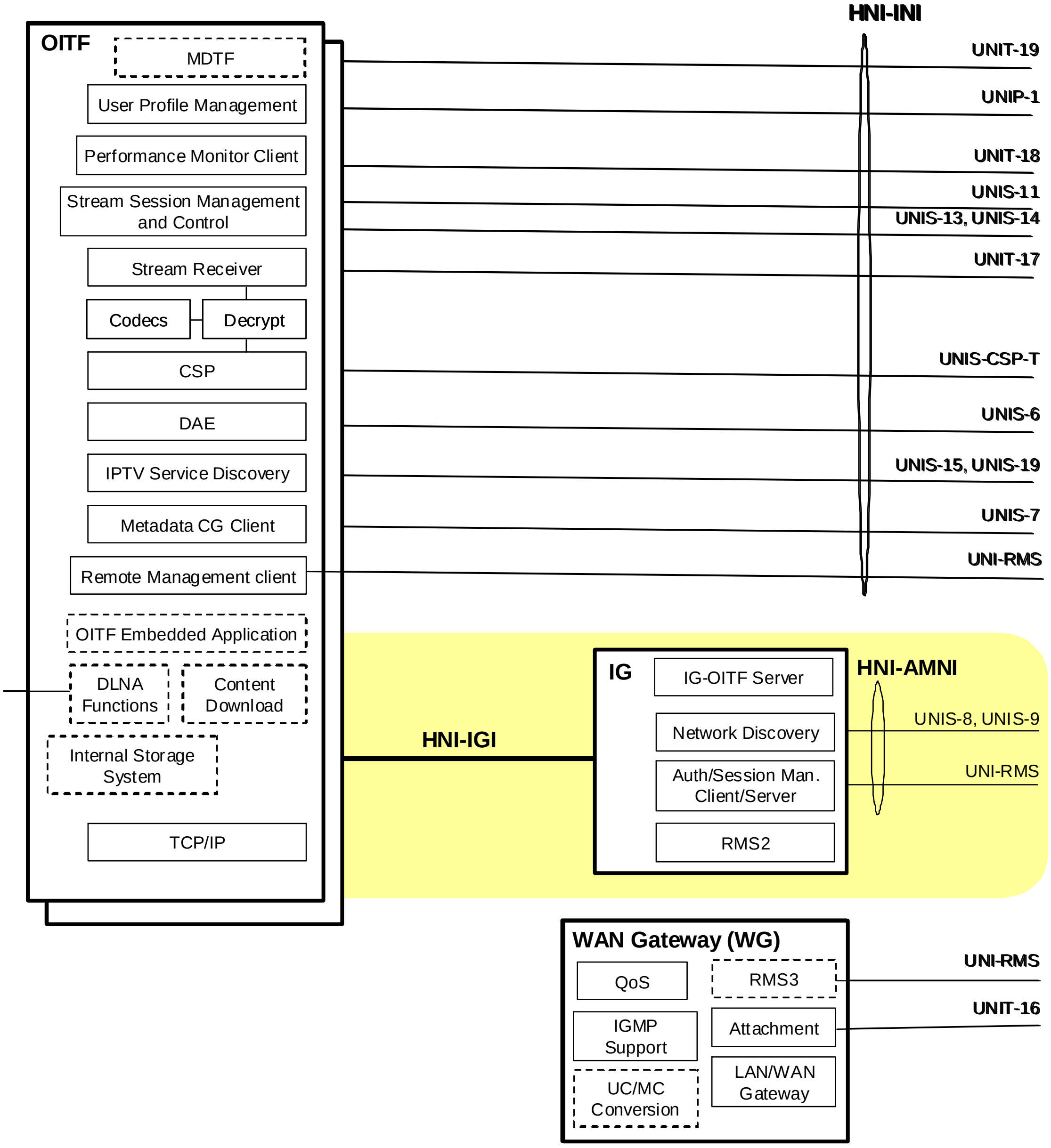


Figure 5-5: OITF and IG

The IG depicted in

Figure 5-5 includes the following additional functions:

IMS Gateway (IG)

Authentication/Session Management Client/Server: Responsible for subscriber authentication and any session management required for managed networks (e.g., managed IPTV services and person-to-person communication services). The authentication performed by this function is (re-)used for Content and Service Protection (CSP) purposes.

The Authentication/Session Management client/server interacts with the network servers through the UNIS-8 interface

This function includes the implicit connectivity admission control (CAC) request for the WAN side. No explicit CAC function is required on the LAN side.

IG-OITF Server: The IG-OITF server exposes authentication and session management client/server functionalities to the OITF for managed IPTV services and blended person-to-person communication application support (e.g., caller id display, messaging etc.) via HTTP and/or other protocols as required. If required, the interaction between the IG-OITF Server and the OITF may result in a UI on the OITF display or the delivery of execution script(s) to the DAE function on the OITF.

RMS2: Client application for remote management functions in a managed environment. It provides a standard interface for provisioning and assurance tasks on managed OIF devices with the IG function (i.e. TR-069 CWMP remote management protocol [Ref 1], plus TR-104 [Ref 29] IMS data model with possible extensions). It includes functions for configuration management, firmware upgrade, troubleshooting/diagnostics, performance management and monitoring of IMS/SIP services.

Network Discovery: Network discovery function is responsible for the discovery of and attachment to an IMS service provider.

5.3.1.3 OITF, IG, AG and CSPG

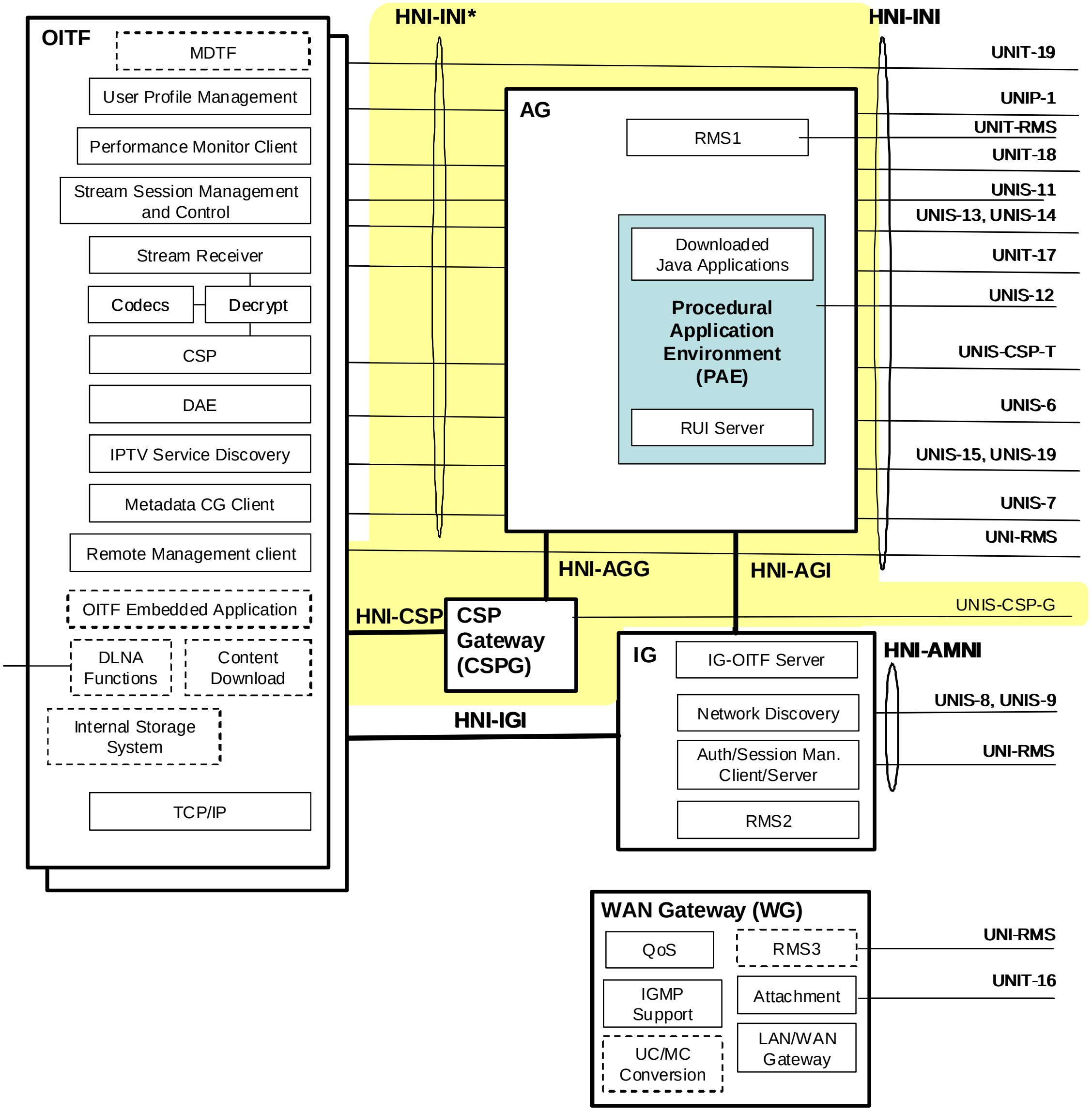


Figure 5-6: All HN Functional entities

A residential network with the addition of the optional Application Gateway and the optional CSP Gateway functional entities is depicted in Figure 5-6. This represents a residential network with all the HN functional entities. The AG and CSPG are independent optional functional entities that may be required in a specific residential network configuration. The following additional functions are identified.

Application Gateway (AG)

Procedural Application Environment (PAE): A local procedural language execution environment based on Java Connected Device Configuration (CDC) [Ref 34] for IPTV Service Provider specific downloaded applications. If required, these applications can present a UI via the CEA-2014 [Ref 2] based Remote UI function on the OITF's DAE. When the PAE is deployed in a device with local graphics rendering (e.g., combined with an OITF), these applications also can also directly access that local graphics system.

The definition of the full capabilities of the PAE is within the scope of the Forum's specifications. The specification of the Service Provider specific applications that are downloaded and executed in the environment are outside of the scope of the Forum's specifications.

The PAE is a multipurpose execution environment capable of supporting many IPTV-specific and general services. These capabilities include support of the following service provider specific applications:

- **Media Control**: Enables the Service Provider to locally intercept the media stream (media, control, CSP) for the purpose of adding or inserting content generated or stored in the AG into that media stream. The operation of Media Control shall be under the control of Applications running in the PAE via defined APIs.
  Note that for protected content, this is only possible when the AG and the CSPG are combined in the same device and that the Release 1 specifications do not define routing media content (for the purposes of media control) via an AG which is not also a CSPG
- **CG**: Client with the following functions:
  - Discovery and description of available services and content.
  - At least one of:
    - Presentation of an CG on the OITF via the DAE
    - Passing all or some subset of the metadata to the "Metadata CG client" on the OITF, depending on the policy of either the Service Platform Provider or the IPTV Service Provider.
      Note that this is not addressed in the Release 1 specifications.
    - When present, this application terminates the UNIS-7 interface in addition to the CG application client in the OITF, which also directly handles the UNIS-7 interface.
- **IPTV Service Discovery:** Client with the following functions:
  - Discovery of available service providers.
  - Discovery and description of available services and content.
- **Fully blended communication services**: Possibly requiring additional hardware to support advanced applications such as video telephony. The HNI-AGI interface allow applications in the AG implementing advanced communication services to access the Authorization and Session Management functions in the IG.
- **RUI Server**: This function enables applications running in the PAE to serve declarative language applications running on the DAE in the OITF.
- **Proprietary or non-standard content download protocols:** Implementation of proprietary, non-standard or other service provider-specific protocols in a PAE application.

RMS1: Client application for remote management functions in a managed environment. It provides a standard interface for provisioning and assurance tasks on managed OIF devices with the AG function (i.e. TR-069 CWMP remote management protocol [Ref 1], plus TR-135 [Ref 30]/TR-140 [Ref 31] IPTV/storage data model with possible extensions). It includes functions for configuration management, firmware upgrade, troubleshooting/diagnostics, performance management and monitoring of streaming services.

CSP Gateway (CSPG)

The CSP Gateway is required when a gateway centric approach to service and content protection is deployed as an alternative to the Marlin based CSP functions of the OITF. A secure authenticated channel is used between the CSPG and the OITF.

5.3.2 Handling QoS in the Residential Network

The QoS function in the WAN gateway is responsible for the QoS marking (e.g., DSCP, Ethernet priority) into and out of the residential network. All nodes in the residential network are responsible for marking the appropriate priority of originating traffic.

5.3.3 Multicast Handling in modem gateway router

Modem gateway router includes transport related functionality such as LAN handling, IP multicast support, etc. IPTV services require additional functionality to be supported in order to ensure efficiency in the home LAN environment.

5.3.3.1 Multicast and the Home LAN

It is expected that scheduled content services will use IP multicast technology to deliver A/V streams. Although IP multicast is efficient in the Network Provider domain, it will cause some issues in Residential network environment, such as

- Flooding to unnecessary segments

  Gateway routers broadcast incoming multicast packets to all ports, resulting in unnecessary packets being delivered to endpoints that are not listeners for that or any multicast stream, and must discard them. This situation is depicted in Figure 5-7: Example of flooding issue

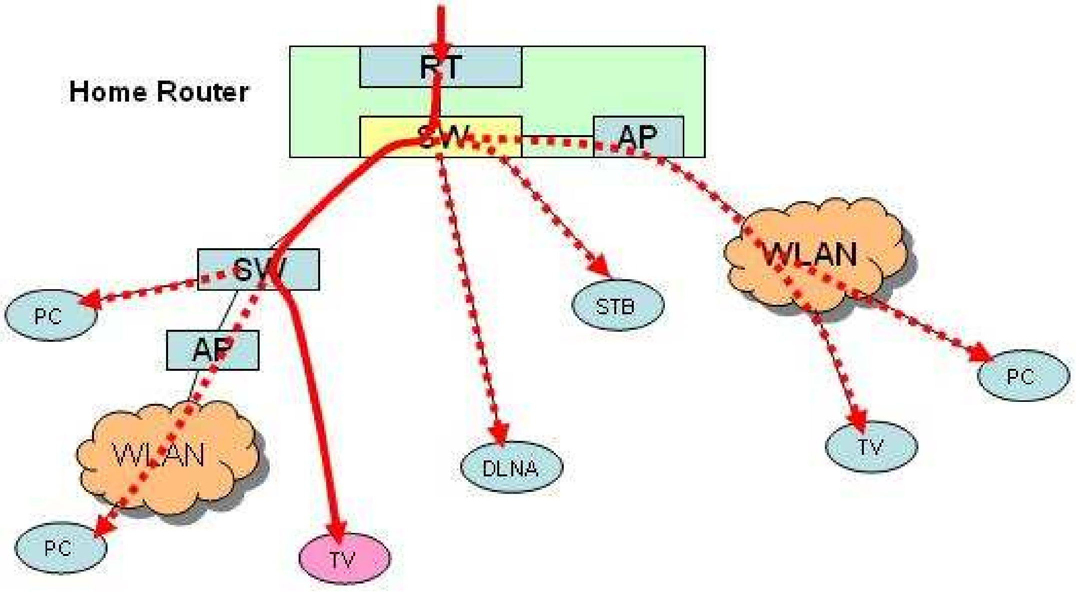


Figure 5-7: Example of flooding issue

  IGMP snooping in the switching function of the home gateway router will solve this issue to some extent. But if there is a secondary switch in the residential network which does not support IGMP snooping, the same issue still remains, although its severity has been reduced.

- Low efficiency and unreliability of multicast on Wireless networks (802.11 WLAN) [Ref 7]

  Multicast frames can not be transmitted at as high a rate as unicast frames. Also, the reliability of multicast is low due to the lack of retransmission mechanisms in Layer 2.

  To remedy this problem, it is necessary to perform multicast to unicast conversion at the home entry point. The conversion will be done at Layer 2 or Layer 3 by snooping IGMP messages [Ref 8] and managing the membership of multicast listeners.

In this release of the architecture, support of IGMP snooping and IGMP proxy [Ref 9] is mandatory to avoid flooding of unnecessary segments.

5.3.3.2 Local Multicast within the Gateway Router

It is mandatory for home routers compliant to this architecture to support local multicasting to avoid the consumption of any additional bandwidth in the last mile when multiple end points are watching the same stream. IGMP snooping can solve that issue by dropping IGMP JOINs for streams that are already available, and ensuring that these streams are replicated locally and delivered to these end points.

5.3.4 Deployment Options

This section describes the allowable deployment options in the residential network, and the services supported by each deployment option.

Each of the OITF, IG, AG and WG functional entities may be deployed as separate physical devices in the residential network, or in combinations as described in this section.

5.3.4.1 Services Available in the Residential Network

Table 4 shows the services available the residential network for each combination of functional entities.

Functional Entities deployed in the residential network				**Services available**
WG	**OITF**	**IG**	**AG**	
X	X			Unmanaged network services only are available. DAE applications can be deployed.
X	X	X		Managed network and unmanaged network services are available. DAE applications can be deployed.
X	X	X	X	Managed network and unmanaged network services are available. DAE and PAE applications can be deployed.
X	X		X	[This deployment option is not defined by this version of the specification] Unmanaged network services are available. DAE and PAE applications can be deployed.

Table 4: Services from Functional Entities

Note that the CSP Gateway functional entity is not shown in this table. Details of the CSP Gateway deployment can be found in section 5.3.4.3

5.3.4.2 Deployment Examples

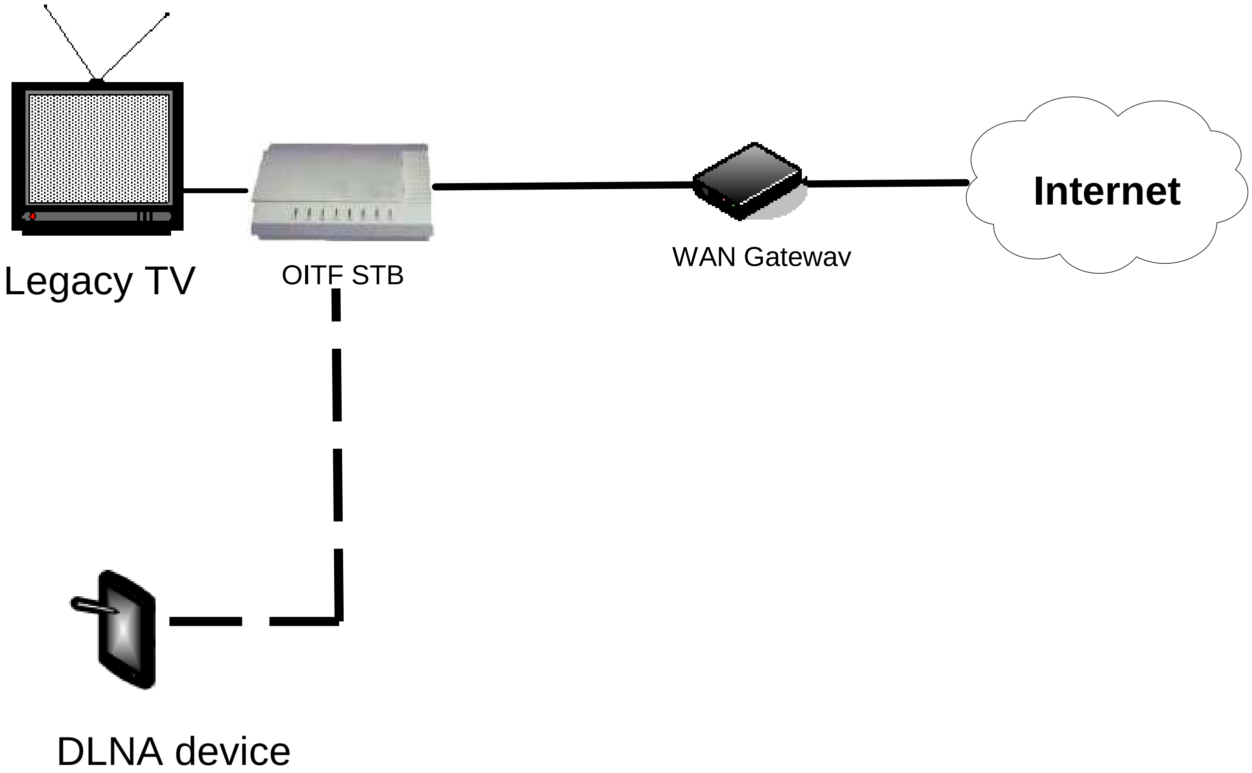
This section outlines some practical deployment scenarios. It is not an exhaustive list of all possible deployments, but examples that illustrate how services may be deployed using new and legacy equipment.

The following terminology is used in this section:

Legacy TV	A television without OIF or DLNA capabilities. Connection to such a television is via, for example, HDMI or SCART.

In the diagrams, dashed lines represent optional connections.

5.3.4.2.1 OITF STB

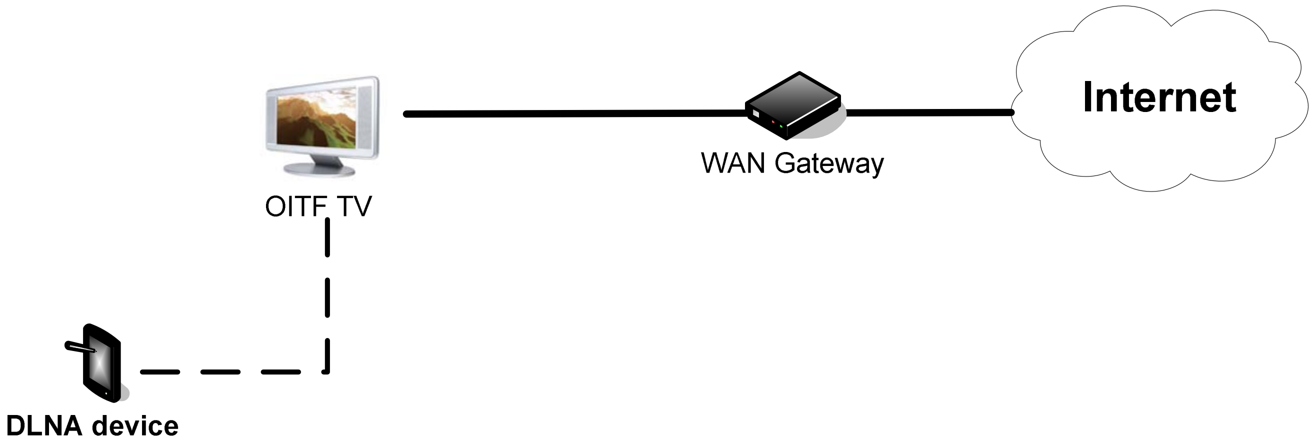


This deployment supports the consumption of unmanaged services using a legacy TV. The following devices are deployed.

- A WAN Gateway: This is a standard modem/router, providing access to an unmanaged network via an ISP.
- OITF STB: A set top box implementing the OITF and connecting to a legacy TV via, for example, HDMI or SCART.
- Legacy TV: A television without OITF or DLNA capabilities.

Optionally, the OITF STB may act as a DLNA DMS to make OIF services available to DLNA devices. It may also act as a DLNA DMP to access content from other DLNA devices on the residential network.

5.3.4.2.2 OITF TV

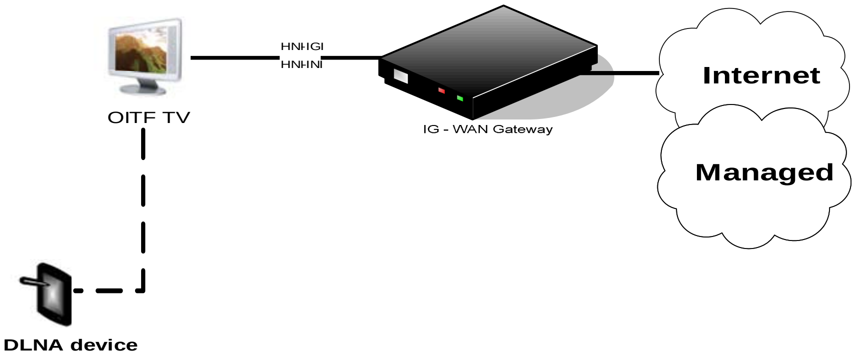


This deployment supports unmanaged services without the need for an additional set top box. The following devices are deployed.

- A WAN Gateway: This is a standard modem/router, providing access to an unmanaged network via an ISP.
- OITF TV: A television including an OITF.

Optionally, the OITF TV may act as a DLNA DMS to make OIF services available to DLNA devices. It may also act as a DLNA DMP to access content from other DLNA devices on the home network.

5.3.4.2.3 Combined IG - WAN Gateway with OITF TV

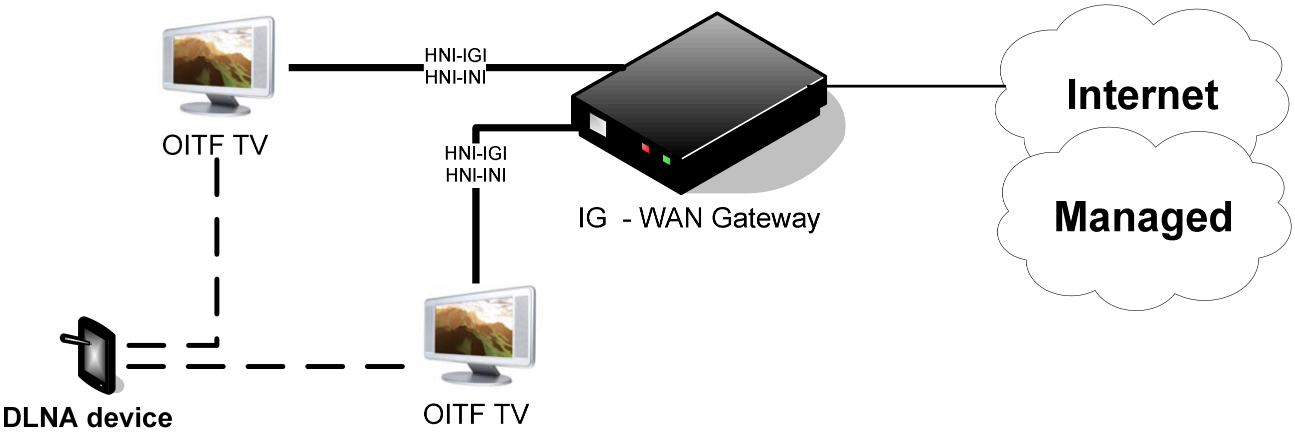


This deployment supports both managed and unmanaged services, with DAE applications. The following devices are deployed:

- Combined IG and WAN Gateway: A single physical device including an IG and modem/router functionality.
- OITF TV: This is an OITF TV, as described in this document.

Optionally, the OITF TV may act as a DLNA DMS to make OIF services available to DLNA devices. It may also act as a DLNA DMP to access content from other DLNA devices on the home network.

5.3.4.2.4 Combined IG – WAN Gateway with multiple OITF TVs

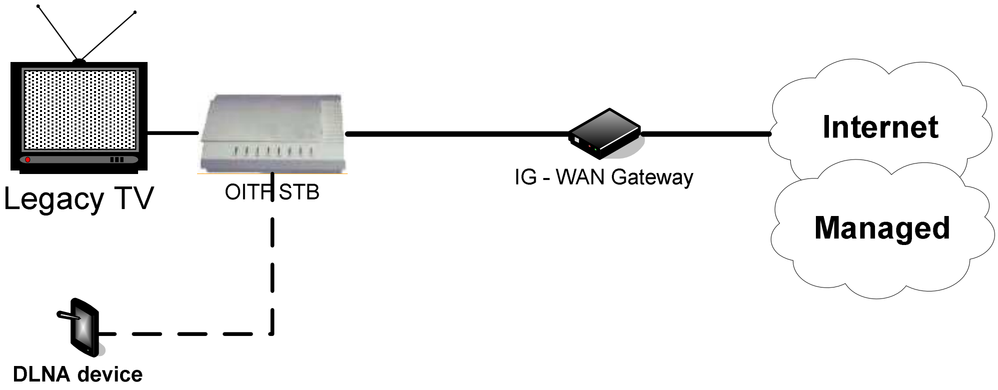


This deployment supports both managed and unmanaged services, with DAE applications. The following devices are deployed:

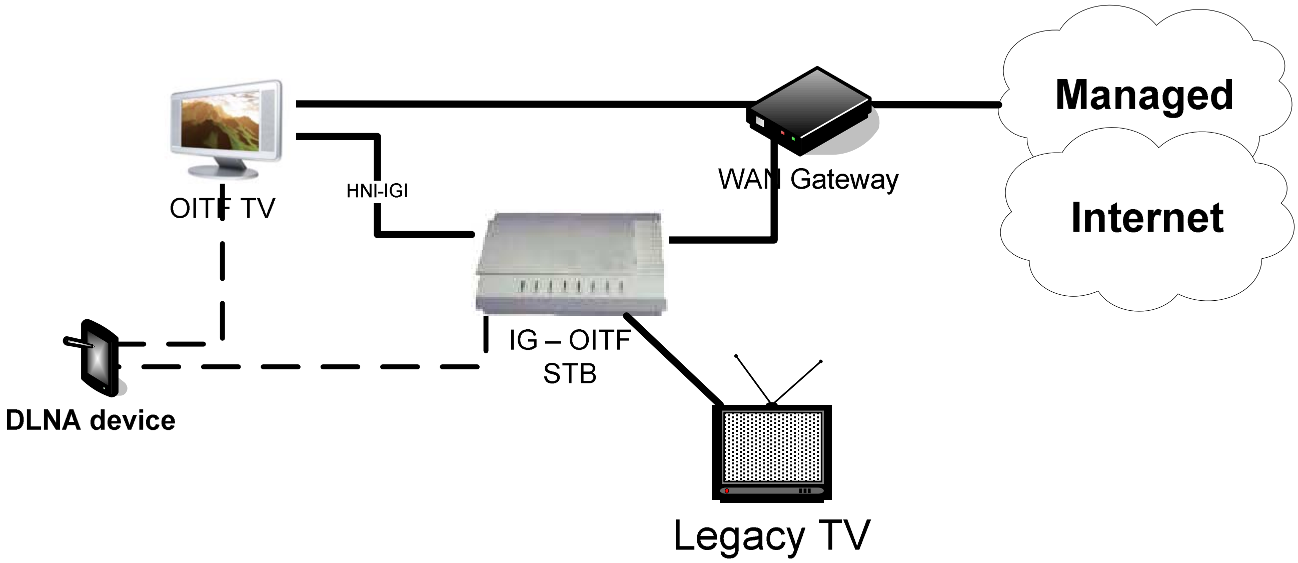
- Combined IG and WAN Gateway: A single physical device including an IG and modem/router functionality.
- OITF TVs: These are OITF TVs, as described in this document.

Optionally, either OITF TV may act as a DLNA DMS to make OIF services available to DLNA devices. It may also act as a DLNA DMP to access content from other DLNA devices on the home network.

Note that one or both OITFs may be deployed in an STB connected to a legacy TV, as shown below, instead of being embedded in a TV.



5.3.4.2.5 Combined IG-OITF STB and Multiple OITFs

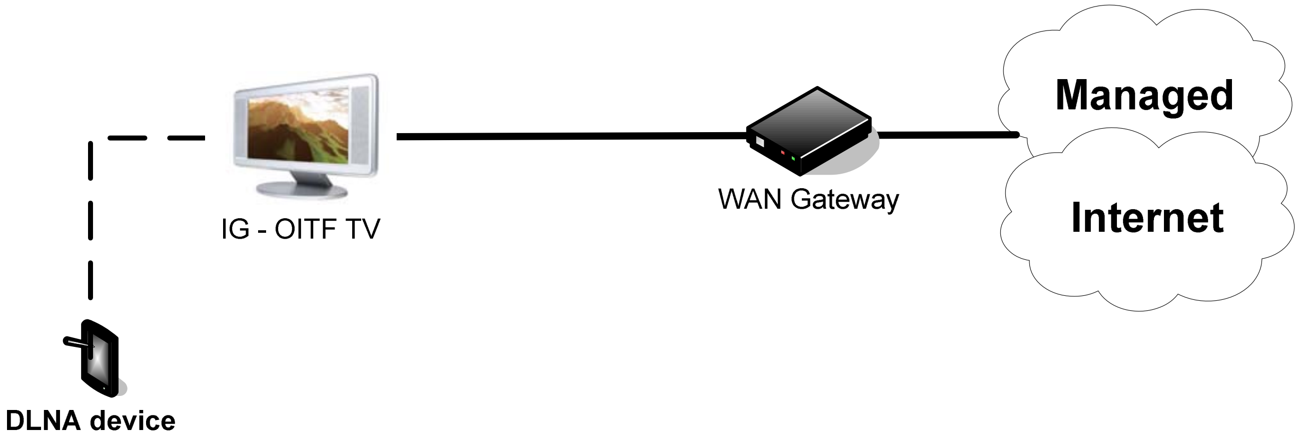


This deployment supports both managed and unmanaged services, with DAE applications, presented on an OITF TV and a legacy TV. The following devices are deployed:

- A WAN Gateway
- Combined IG and OITF STB: A set top box including IG and OITF functionality that exposes HNI-IGI to other OITFs in the residential network. It connects to the legacy TV using some non-OIF specified mechanism, such as HDMI or SCART.
- OITF TV: This is a TV containing an OITF.

Optionally, the OITF TV and IG-OITF STB may act as a DLNA DMS to make OIF services available to DLNA devices. It may also act as a DLNA DMP to access content from other DLNA devices on the home network.

5.3.4.2.6 Combined IG – OITF TV



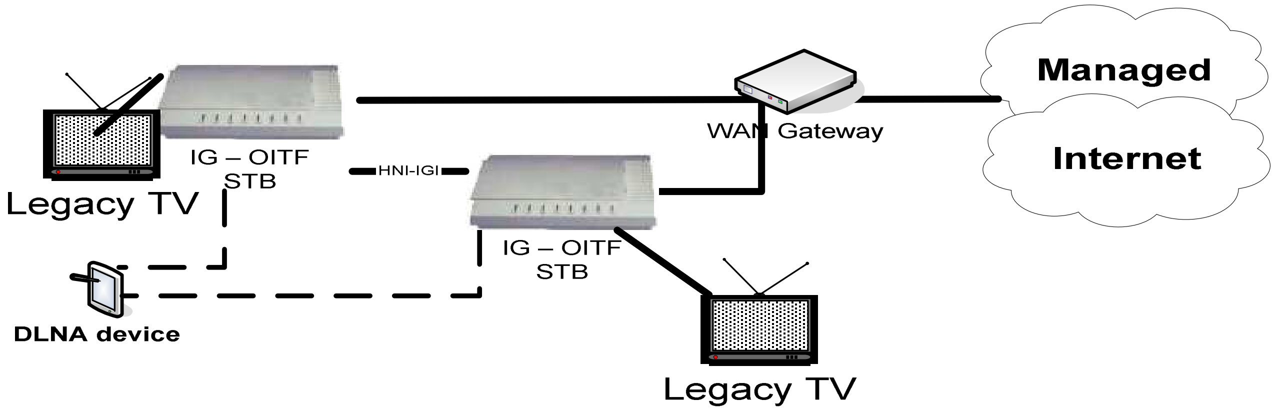
This deployment supports both managed and unmanaged services, with DAE applications, presented on an OITF TV. The following devices are deployed:

- A WAN Gateway.
- Combined IG and OITF TV: A TV including both IG and OITF functionality.

Optionally, the IG-OITF TV may act as a DLNA DMS to make OIF services available to DLNA devices. It may also act as a DLNA DMP to access content from other DLNA devices on the home network.

Note that the IG inside the TV may be used by external OITFs to access managed services.

5.3.4.2.7 Multiple IG – OITF STBs



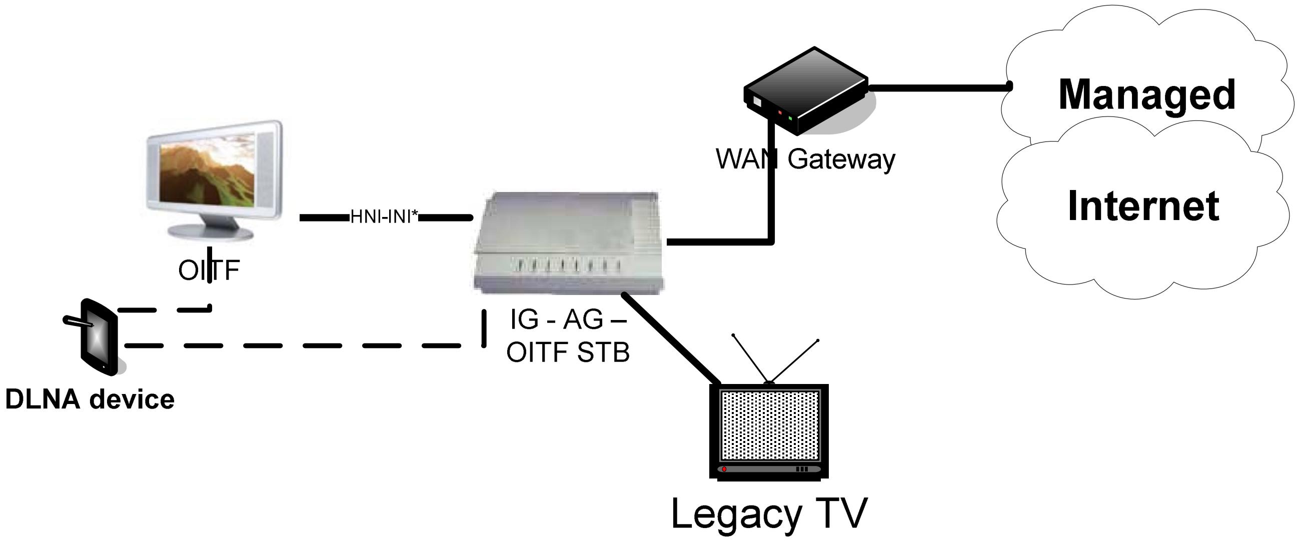
This deployment supports both managed and unmanaged services, with DAE applications, presented on multiple legacy TVs. The following devices are deployed:

- A WAN Gateway.
- Two combined IG-OITF STBs: STBs including both IG and OITF functionality.

Only one IG can be active in the residential network at any one time. This limitation may be relaxed in a future specification.

Optionally, each IG-OITF TV may act as a DMS to make OIF services available to DLNA devices. They may also act as a DMP to access content from other DLNA devices on the home network.

5.3.4.2.8 Combined IG-AG-OITF STB and OITF TV

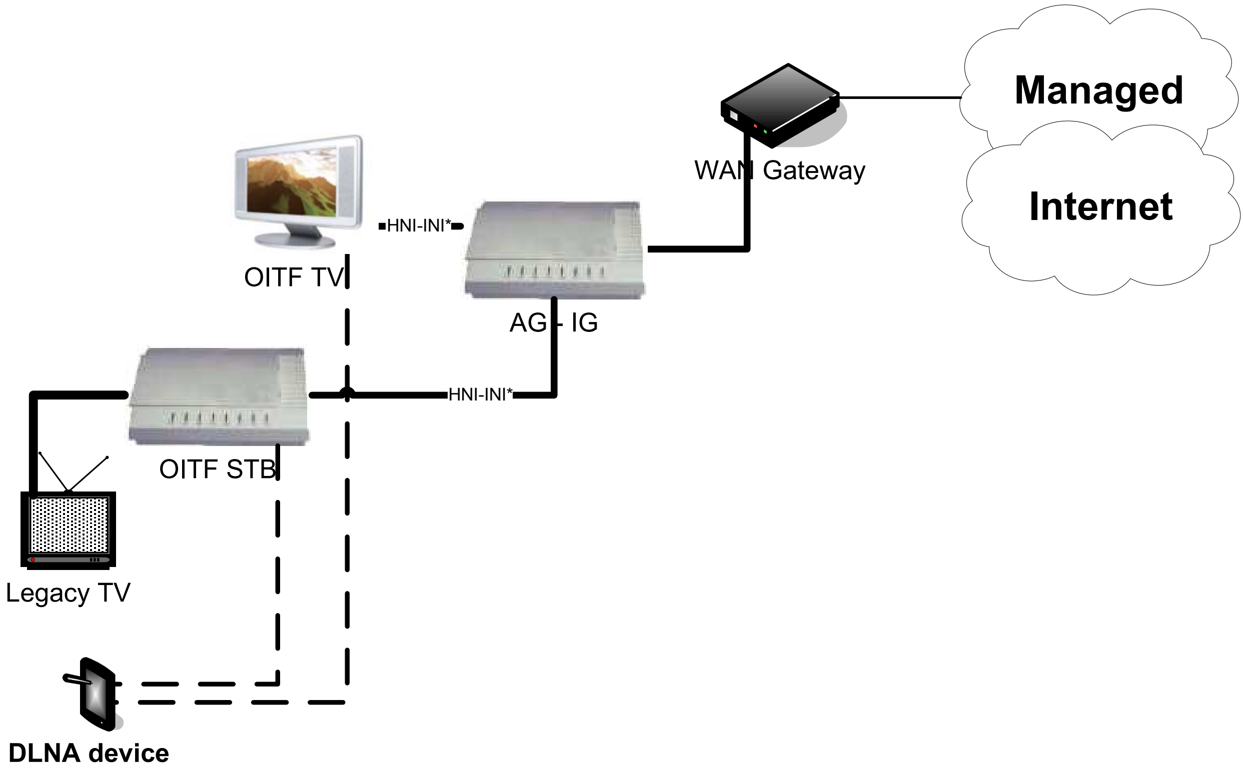


This deployment supports both managed and unmanaged services, with DAE and PAE applications, presented on an OITF TV and a legacy TV. The following devices are deployed:

- A WAN Gateway.
- Combined IG, AG and OITF STB: A set top box including IG, AG and OITF functionality, that exposes HNI-INI* to other OITFs in the residential network. It connects to the legacy TV using some non-OIF specified mechanism, such as HDMI or SCART.
- OITF TV: This is a TV containing an OITF.

Optionally, the IG-AG-OITF STB or the OITF TV may act as a DLNA DMS to make OIF services available to DLNA devices. They may also act as a DLNA DMP to access content from other DLNA devices on the home network.

5.3.4.2.9 Combined AG-IG with multiple OITFs

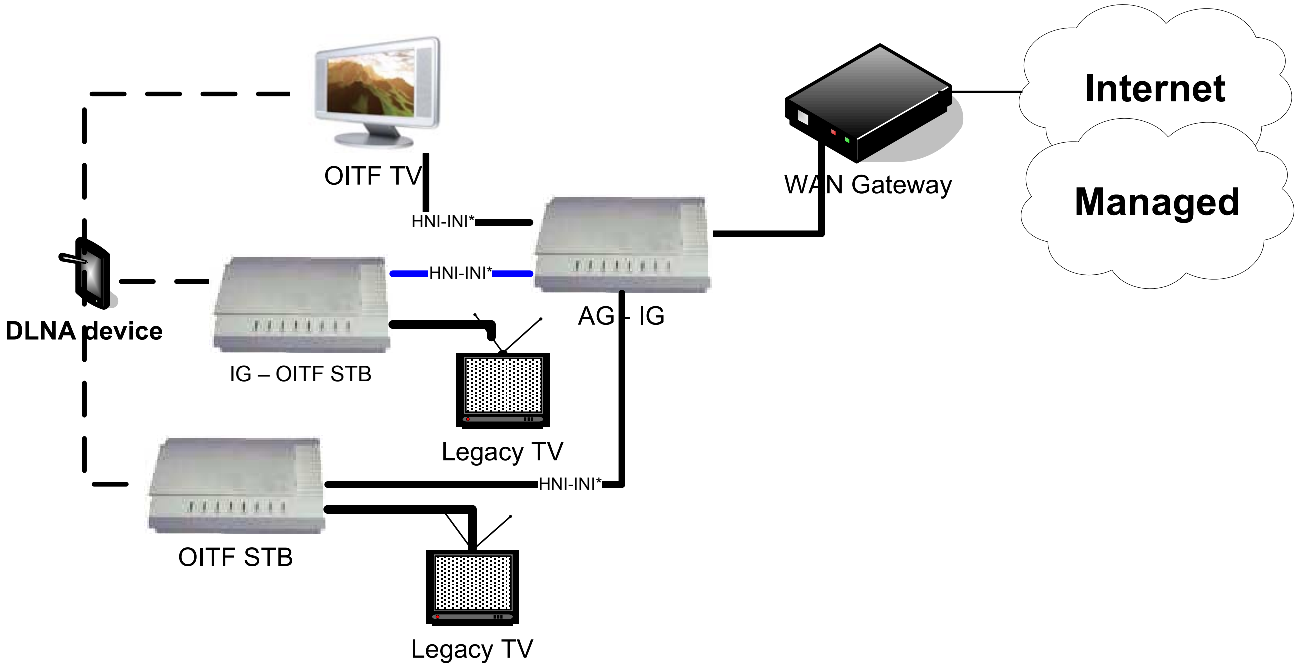


This deployment supports both managed and unmanaged services, with DAE and PAE applications, presented on an OITF TV and a legacy TV. The following devices are deployed:

- A WAN Gateway.
- Combined AG-IG device: A device including both IG and AG functionality, that exposes HNI-INI* to OITFs in the residential network.
- OITF STB: A set top box containing an OITF. It connects to the legacy TV using some non-OIF specified mechanism, such as HDMI or SCART.
- OITF TV: A TV containing an OITF.

Optionally, the OITF STB or the OITF TV may act as a DLNA DMS to make OIF services available to DLNA devices. They may also act as a DLNA DMP to access content from other DLNA devices on the home network.

5.3.4.2.10 AG-IG, OITF-IG, Multiple OITFs

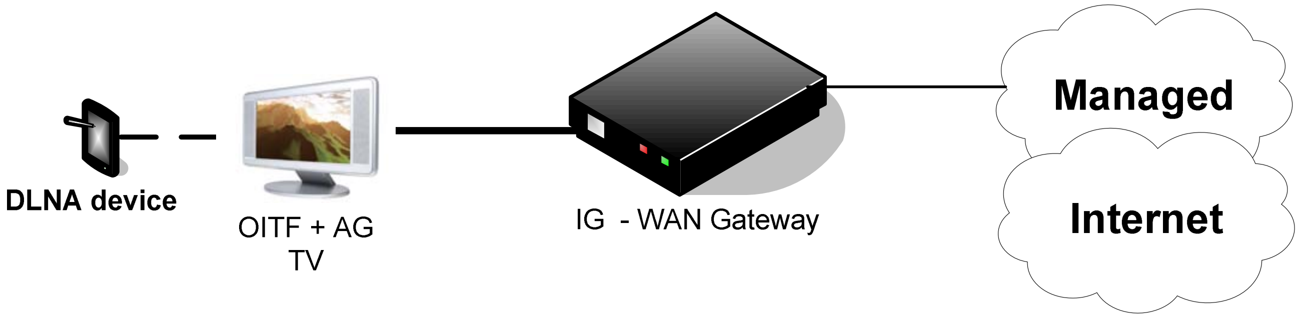


This deployment supports managed and unmanaged services, and DAE and PAE applications. The following devices are deployed:

- A WAN Gateway.
- Combined AG-IG device: A device including both IG and AG functionality, that exposes HNI-INI* to OITFs in the residential network.
- OITF STB: A set top box containing an OITF. It connects to the legacy TV using some non-OIF specified mechanism, such as HDMI or SCART.
- IG-OITF STB: A set top box containing both an IG and an OITF.
- OITF TV: A TV containing an OITF.

In this deployment, there are multiple IGs. Only one IG can be active in the residential network at any point in time. The ISIM application must always be in the AG-IG in this case.

5.3.4.2.11 Combined OITF-AG TV and IG-WAN Gateway



This deployment supports managed and unmanaged services, and DAE and PAE applications. The following devices are deployed:

- Combined IG-WAN Gateway: A single physical device including an IG and WAN Gateway functionality.
- Combined AG-OITF TV: A TV including both an OITF and an AG.

Optionally, the OITF-AG TV may act as a DLNA DMS to make OIF services available to DLNA devices. It may also act as a DLNA DMP to access content from other DLNA devices on the home network

5.3.4.3 CSP Gateway

The optional CSP Gateway (CSPG) functional entity implements proprietary content and service protection and delivers content to OITFs using a secure authenticated channel between the CSPG and the OITF.

Some possible deployment scenarios include:

- An IG and CSP Gateway combined device
- An AG, IG and CSP Gateway combined device.
- An AG and CSP Gateway combined device

Note that the media control features of the AG are only possible for protected content when the AG and CSP Gateway are combined in one device.

Note that the Release 1 specifications do not define routing media content (for the purposes of media control) via an AG which is not also a CSPG

5.3.5 Residential Network Reference Points

- **HNI-INI**: This is a group of reference points directly connected to the OITF to provide application layer protocols common to both managed and unmanaged models. If an AG function is deployed, the AG may terminate HNI-INI in addition to the OITF as described in section 5.3.1.3. The HNI-INI consists of the following UNI reference points.
    - **UNIP-1** (to “User Profile Management”)
    - **UNIS-13** (to “Stream Session Management and Control”)
    - **UNIS-11** (to “Stream Session Management and Control”)
    - **UNIS-CSP-T** (to “CSP”)
    - **UNIS-6** (to “DAE”)
    - **UNIS-7** (to “Metadata based Content Guide client”)

  - **UNIT-17** (to “Stream receiver”)
  - **UNIS-14** (to “Stream Session Management and Control”)
  - **UNIS-15** (to “Service Discovery”)
  - **UNIT-18** (to “Performance Monitor Client”)

- **HNI-INI*:** This interface is a group of reference points between the OITF and AG which supports the adaptation of the IPTV services to the OITF. Where applicable, this interface uses the same protocols as HNI-INI, as follows: the UNIS-6 reference point always applies between the OITF and AG. The following reference points may apply when the AG includes A/V media storage - UNIS-11, UNIT-17 and UNIT-18. Use of the remaining reference points from HNI-INI between an OITF and an AG is not defined in the Release 1 specifications. Additionally, the HNI-INI* includes the device discovery mechanisms.

- **HNI-IGI**: This interface is between the OITF and IG and provides, to the OITF, access to IG functions for the adaptation to IPTV services on managed networks. The HNI-IGI includes device discovery mechanisms.

- **HNI-AGI:** This interface is between the IG and AG and provides. To the AG, access to IG functions for the adaptation to IPTV services in managed networks. The HNI-AGI includes device discovery mechanisms.

- **HNI-AMNI**: This interface is between the IG and the network and includes the reference points that are required in addition to the HNI-INI reference points, to deliver managed services.

- **HNI-CSP**: This interface is between the OITF and the CSPG and allows the OITF to access CSPG functions for the conversion from a content and service protection solution to a secure authenticated channel between the CSPG and the OITF..

- **HNI-AGC**: This interface allows access to encryption keys.

5.4 QoS Framework Architecture Description

The QoS framework is responsible for policy-based transport control in the access and core networks, and . includes procedures and mechanisms that handle resource reservation and admission control for both unicast and multicast

The Resource and Admission Control (RAC) [Ref 12] is the building block responsible for these functions.

The RAC is able to interact with the following three main architectural blocks:

- Authentication and Session Management: RAC receives resource reservation requests and output notifications the status of requests

- Transport Processing Functions: RAC enforces policies, receives resource reservation requests and manages the network status

- Network Attachment: RAC receives the subscriber access profile and location information

The RAC supports QoS resource reservation mechanisms triggered in two ways:

- “Push” mode: the RAC pushes traffic policies to the transport processing functions on receipt of a request for resource reservation coming from the Authentication and Session Management

- “Pull” mode: traffic policies are “pulled” by the transport functions from the RAC on receipt of resource requests coming from the Transport Processing Function (e.g. in case of IGMP/PIM) [Ref 10] [Ref 11]

The Push and Pull models and related mechanisms are coordinated by the RAC, to ensure the appropriate policy enforcement for both unicast and multicast services (see Appendix E for details).

5.4.1 RAC functional description and deployment options

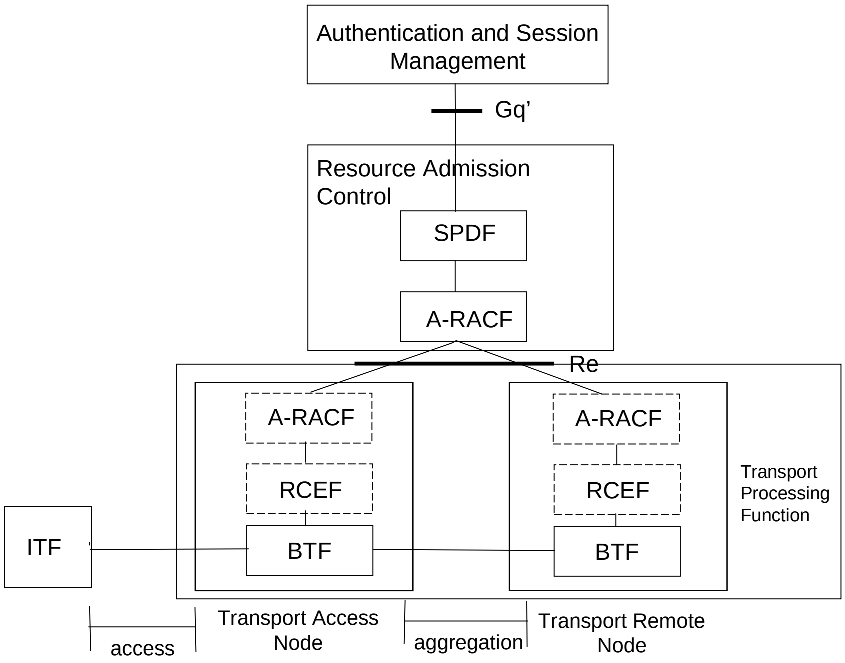


Figure 5-8: Resource and Admission Control Architecture

The RAC functional entities are:

- A-RACF (Access Resource Admission Control Function): performs admission control and derives the traffic policies that are installed in the RCEF.
- SPDF (Service-based Policy Decision Function): provides a single point of contact for the Authentication and Session Management FE to receive resource reservation requests and acts as a final Policy Decision Point for Service-Based Policy control.

The Transport Processing Functions involved in processing unicast and multicast flows are:

- BTF (Basic Transport Function): sends and receives IGMP and PIM messages; and replicates multicast flows;
- RCEF (Resource Control Enforcement Function): enforces traffic policies and builds and forwards admission control requests to the A-RACF;

To maximize performance a distributed architecture is possible; in particular, depending on operator policy, the A-RACF may be located in any Transport Processing Function node. All Transport Processing Function Nodes have the following deployment options:

- BTF only; in this case policies are not enforced at the Transport Node;
- BTF + RCEF; in this case a centralized resource and admission control approach is used;
- BTF + RCEF + A-RACF; in this case a distributed resource and admission control approach is used;

The interfaces between the functional entities are:

- RCEF – A-RACF: based on the same protocol as used between the Authentication and Session Management and the Resource and Admission Control Function, i.e. Diameter [Ref 27]. The RCEF - BTF interface can be considered an internal Transport Processing Functions interface.

- A-RACF – A-RACF: Inter A-RACF interface when multiple A-RACFs are present. One A-RACF could delegate the control of a resource to another A-RACF through this interface.

A more detailed description of the RAC behaviour, with examples of specific deployment scenarios, is provided in Appendix E.

6. High Level Signalling Flows (Informative)

Many of the signalling flows in this chapter have specific protocol choices. It should be noted that these are only examples.

6.1 Network Attachment

Network attachment aims at providing IP addresses and configuration information to elements in the Consumer Domain prior to any other action regarding IPTV services. The provision and management of IP addresses has two main aspects.

IP address management within the Consumer Network: This deals with the attachment of the IG, AG and OITF to the WAN Gateway. The WAN Gateway could act as a DHCP Server and a NAT. This type of attachment allows the IG, AG and OITF to communicate with each other within the residential network.

In the unmanaged network model, this allows the OITF to send and receive messages from the Internet.

IP address management for communication with the Provider Network (Managed Network model only): 2 cases can occur

- The WAN Gateway translates the in-home IP address to an IP address recognizable to the provider's addressing plan. In this case a NAT is needed.
- The WAN Gateway assigns an IP address to the IG, AG and OITF from the managed network's IP addressing pool. In this case no NAT is needed. Configuration information (e.g. DNS server) is obtained directly by the OITF, AG and IG.

> **Note:** It is mandatory that the WAN gateway supports the functionality of translating the in-home IP addresses to IP addresses recognizable to the provider's addressing plan. In this case, a NAT is needed.

6.2 IPTV Service Discovery and Selection

The IPTV Service Discovery is a mechanism to enable an ITF to discover IPTV Service Providers and IPTV services provided by a specific IPTV Service Provider. The procedures of IPTV Service Discovery consists of the following three steps which are consistent with DVB-IP Service Discovery and the discovery information is based on DVB-IP SD&S records for both managed network and unmanaged network .

- **Step 1) Determination of the IPTV Service Provider Discovery entry points:** This procedure is the bootstrap of IPTV Service Discovery, where the ITF finds the entry point(s) of the IPTV Service Provider Discovery functional entity. The mechanisms to determine the entry point(s) can be different between the managed and the unmanaged models. For example, in case of the managed model, the Network Attachment functional entity can provide the IP address to start the IPTV Service Provider Discovery phase.
- **Step 2) IPTV Service Provider Discovery:** This is the procedure where the ITF retrieves the information about each IPTV Service Provider. This information is located at the Service Provider Discovery functional entity, addressed by the entry point(s) found as a result of step 1. This information can be provided either as a web page or based on XML data, such as a DVB-IP Service Provider(s) Discovery Record. It includes the names of IPTV Service Provider(s) and related attributes (e.g. a logo image of the IPTV Service Provider, the means to retrieve IPTV Service Discovery information, etc.). This information will be used by the ITF to perform IPTV Service Provider selection.
- **Step 3) IPTV Service Discovery:** After selecting one IPTV Service Provider from the list obtained in step 2, this procedure allows the ITF to get information about IPTV Services offered by the selected IPTV Service Provider. This information is located at the Service Discovery functional entity. In this step, the term "services" includes linear TV, CoD, nPVR, etc. The IPTV Service Discovery information can be provided either as a web page or as an XML record, such as a DVB-IP Offering record with needed extensions (including the start-up URL for DAE, entry point for the DVB-IP Broadband Content Guide Record and so on).

Note that in the case of 1-to-1 relationship between the Service Platform Provider and the IPTV Service Provider, the IPTV Service Provider Discovery phase (Step 2) would return a single record; therefore, in such a deployment, the subscriber does not have to select the Service Provider and Step 1) could directly provide the address of the IPTV Service Discovery functional entity.

Note that step 2 and step 3 can be repeated without necessarily performing step 1.

When the Service Discovery and Selection Information changes, the IPTV Service Provider Discovery FE or IPTV Service Discovery FE should inform the ITF about this change

The sequence in Figure 6-1 shows a high level call flow for IPTV Service Discovery followed by call flows for IPTV service access, such as retrieving documents for DAE and retrieving content guide metadata. Each call flow can include an optional authentication step to avoid unauthorized access to the IPTV services.

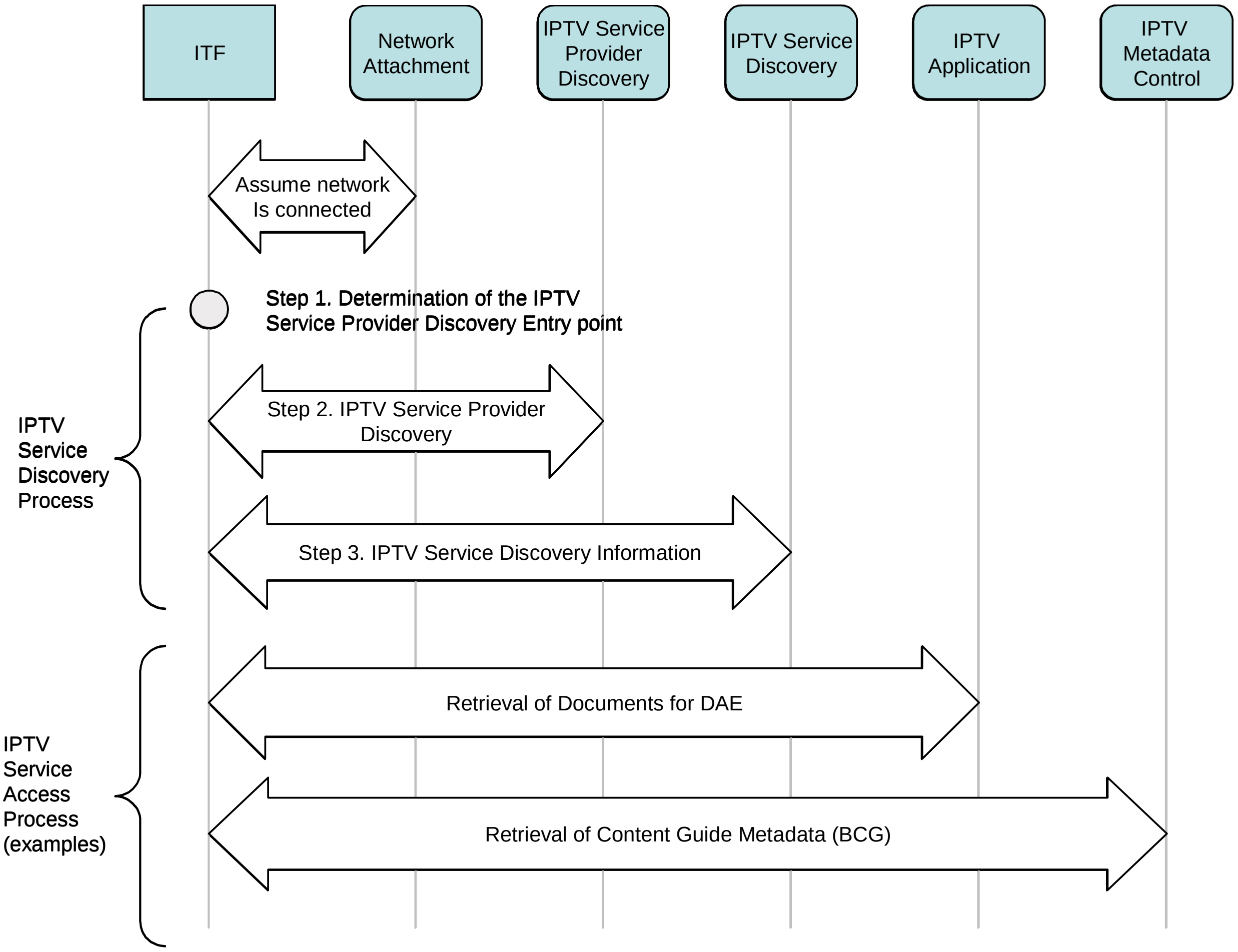

ITF
Network Attachment
IPTV Service Provider Discovery
IPTV Service Discovery
IPTV Application
IPTV Metadata Control
Assume network Is connected
Step 1. Determination of the IPTV Service Provider Discovery Entry point
IPTV Service Discovery Process
Step 2. IPTV Service Provider Discovery
Step 3. IPTV Service Discovery Information
IPTV Service Access Process (examples)
Retrieval of Documents for DAE
Retrieval of Content Guide Metadata (BCG)

Figure 6-1: High level steps in Service Discovery and Service Access

6.2.1 IPTV Service Discovery and IPTV Service Access Procedures for Unmanaged Networks

This section describes the IPTV Service Discovery and Service Access procedures for unmanaged networks. As described in Section 5.3, the minimum set of functional entities needed to access unmanaged IPTV services are the OITF and the WAN Gateway; thus, the IPTV Service Discovery and Service Access procedures for unmanaged network are shown hereafter considering only these entities.

6.2.1.1 High Level Procedure

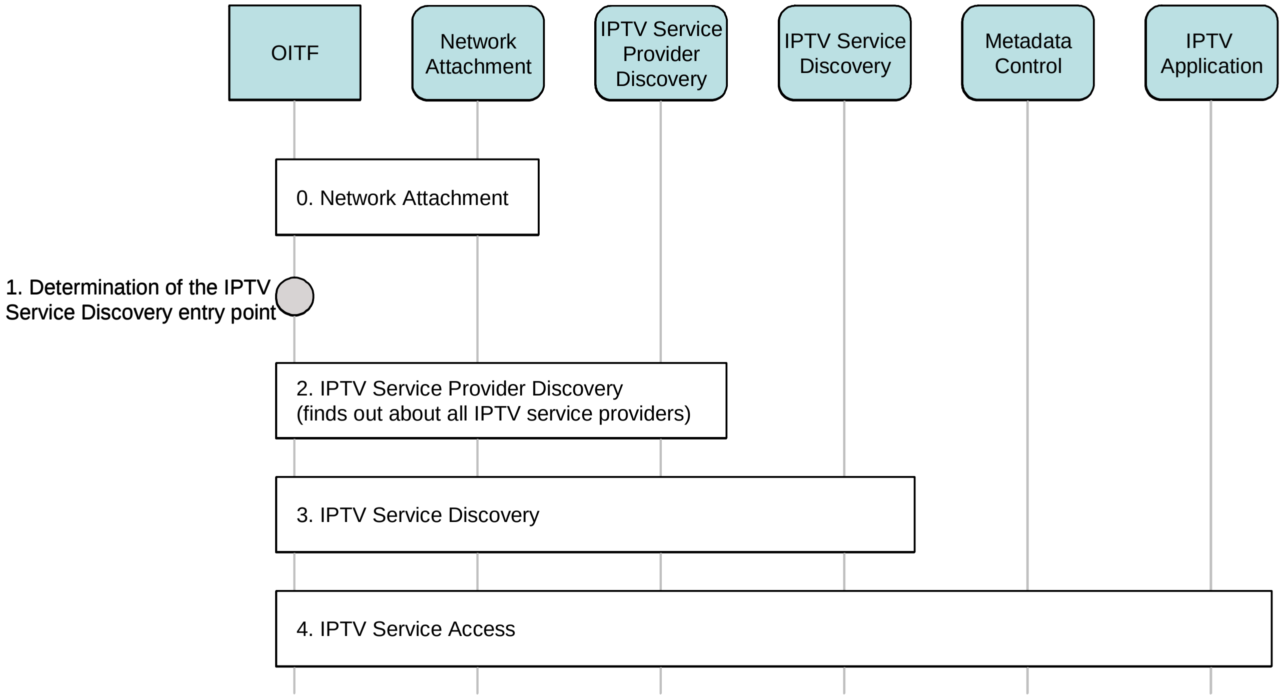

OITF
Network Attachment
IPTV Service Provider Discovery
IPTV Service Discovery
Metadata Control
IPTV Application
0. Network Attachment
1. Determination of the IPTV Service Discovery entry point
2. IPTV Service Provider Discovery (finds out about all IPTV service providers)
3. IPTV Service Discovery
4. IPTV Service Access

Figure 6-2: High level steps for Service Discovery and Service Access for unmanaged networks

The IPTV Service Discovery and IPTV Service Access procedures for an unmanaged network comprise a number of steps, as shown in Figure 6-2:

1. Determination of the IPTV Service Provider Discovery entry point
2. IPTV Service Provider Discovery
3. IPTV Service Discovery
4. IPTV Service Access (e.g. Access to the Content Guide – via metadata or web page)

These steps are described in detail below.

0. Attachment to the network, where the OITF obtains connectivity to the unmanaged network through the WAN Gateway

1. Determination of an IPTV Service Provider Discovery entry point. This is an internal process in the OITF.

2. The OITF initiates the IPTV Service Provider Discovery using this entry point. In this step, the IPTV Service Provider Discovery functional entity provides the list of IPTV Service Providers and information that is used in the next step (e.g. IPTV Service Provider name, IP address, protocols to be used)

3. The OITF initiates the IPTV Service Discovery. In this phase the OITF selects an IPTV Service Provider and obtains the list of IPTV services available from that specific IPTV Service Provider

4. The OITF can select and access an IPTV service, e.g. access the Content Guide.

6.2.1.2 Determination of the IPTV Service Provider Discovery entry points

For unmanaged networks, the OITF determines the entry point(s) with the following options. There is no priority order for these options.

- **Manual**

  The End User manually enters a URL or an IP address/port. The OITF should provide a means to allow users to enter an entry point easily, e.g. bookmark, or default URL and the means by which this is achieved is OITF vendor dependent.

- **Pre-Configured**

  Optionally, all the necessary information can be pre-configured in the OITF.

- **DHCP Configuration**

  Optionally, the OITF retrieves provider discovery entry points via DHCP configuration parameters. This would be provided by the ISP to which the residential network connects.

6.2.1.3 IPTV Service Provider Discovery

The OITF requests the information on the available IPTV service providers from the IPTV Service Provider Discovery functional entity via HTTP(S).

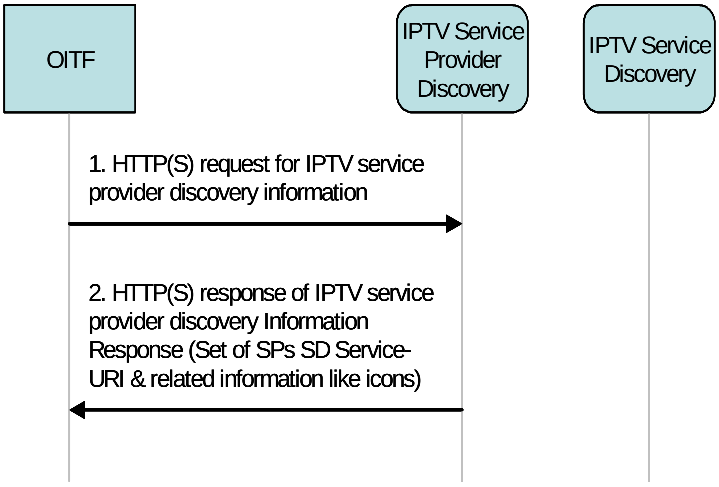

OITF
IPTV Service Provider Discovery
IPTV Service Discovery
1. HTTP(S) request for IPTV service provider discovery information
2. HTTP(S) response of IPTV service provider discovery Information Response (Set of SPs SD Service-URI & related information like icons)

Figure 6-3: IPTV Service Provider Discovery for unmanaged networks

6.2.1.4 IPTV Service Discovery

The Service Discovery Record can be delivered via HTTP(S) as XML data (DVB-IP SD&S Record) or as a Web Page.

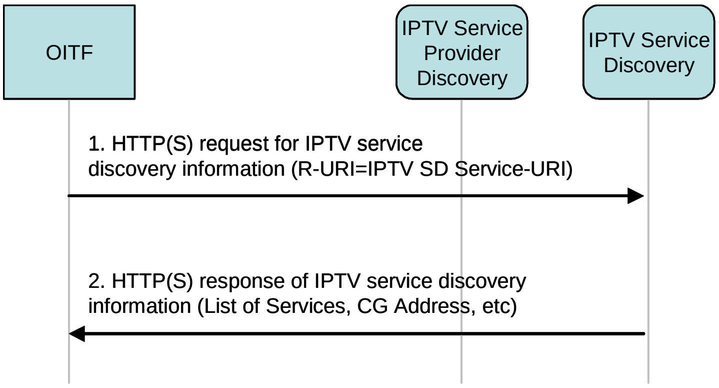

OITF
IPTV Service Provider Discovery
IPTV Service Discovery
1. HTTP(S) request for IPTV service discovery information (R-URI=IPTV SD Service-URI)
2. HTTP(S) response of IPTV service discovery information (List of Services, CG Address, etc)

Figure 6-4: IPTV Service Discovery for unmanaged networks

6.2.1.5 IPTV Service Access

The following figure shows the call flow for obtaining the Content Guide, which is an example of IPTV service access.

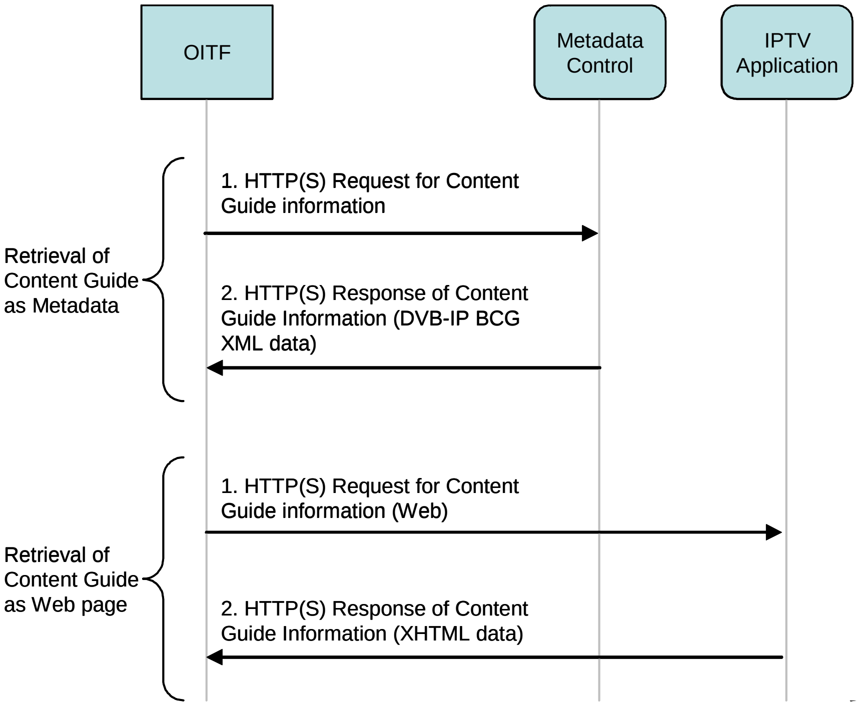

OITF
Metadata Control
IPTV Application
Retrieval of Content Guide as Metadata
1. HTTP(S) Request for Content Guide information
2. HTTP(S) Response of Content Guide Information (DVB-IP BCG XML data)
Retrieval of Content Guide as Web page
1. HTTP(S) Request for Content Guide information (Web)
2. HTTP(S) Response of Content Guide Information (XHTML data)

Figure 6-5: IPTV Service Access for unmanaged networks

6.2.2 IPTV Service Discovery and IPTV Service Access Procedures for the Managed Model

This section describes the IPTV Service Discovery and Service Access procedures for managed networks. As described in Section 5.3, the minimum set of functional entities needed to access the managed IPTV services are the OITF, the IG and the WAN Gateway; moreover, the AG can be introduced as an optional functional entity in some deployment options.

The IPTV Service Discovery and Service Access procedures are shown hereafter, starting from a high-level procedure description and then detailing two cases based on two different deployment options. Section 6.2.2.2 shows the case where just the IG is deployed, while Section 6.2.2.3 describes the case where the AG is also deployed together with the IG.

6.2.2.1 High Level Procedure

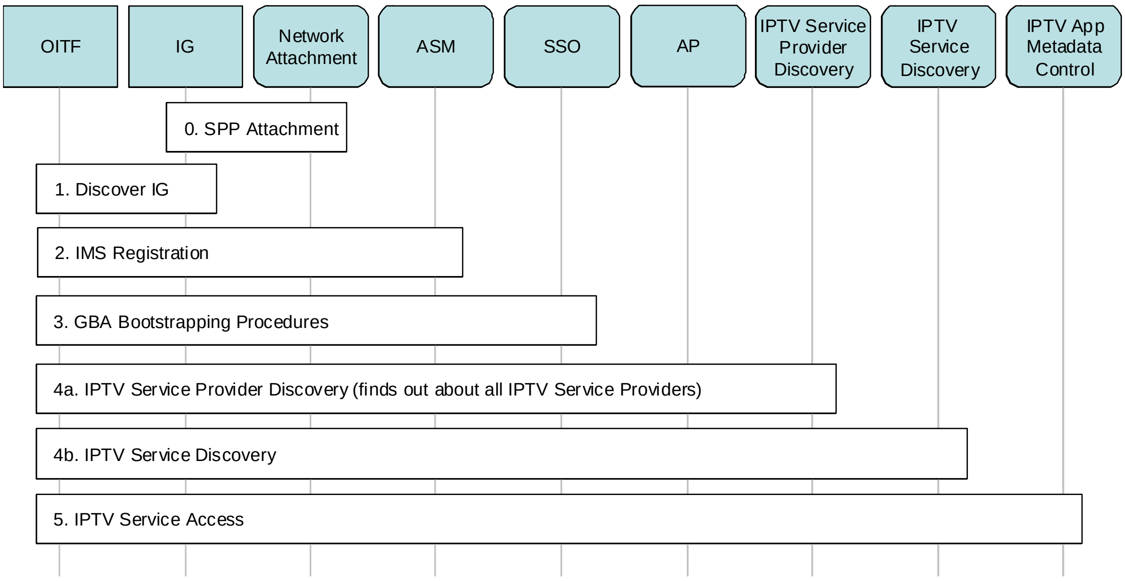

OITF
IG
Network Attachment
ASM
SSO
AP
IPTV Service Provider Discovery
IPTV Service Discovery
IPTV App Metadata Control
0. SPP Attachment
1. Discover IG
2. IMS Registration
3. GBA Bootstrapping Procedures
4a. IPTV Service Provider Discovery (finds out about all IPTV Service Providers)
4b. IPTV Service Discovery
5. IPTV Service Access

Figure 6-6: High level steps for Service Discovery and Service Access for managed networks

The managed network Service Provider Discovery comprises a number of steps as shown in Figure 6-6:

0. Attachment to the Service Platform provider (SPP)

1. Discovery of the IG. The OITF is turned on and obtains the entry point for the IPTV Service Provider Discovery from the IG. The determination of the IPTV Service Provider Discovery entry points can be achieved in a number of ways e.g. pre-configuration of the IG or using a specific event package, the service providers discovery request can be forwarded to the appropriate Service Provider Discovery FE.

2. Registration with the SPP (IMS Registration)

3. GBA bootstrapping procedure

4a. IPTV Service Provider Discovery: The OITF initiates the IPTV Service Provider Discovery. The Service Provider Discovery FE provides the list of IPTV Service Providers and information used for the next step (e.g. IPTV Service Providers' name, IP address, protocols to be used).

4b. IPTV Service Discovery: The OITF initiates the IPTV Service Discovery. In this step, the OITF selects an IPTV Service Provider and obtains from the Service Discovery FE the list of services available from that specific IPTV Service Provider.

5. The OITF can select and access an IPTV service, e.g., access the Content Guide, via metadata or a web page.

In the case where there is a 1-to-1 relationship between the Service Platform Provider and the IPTV Service Provider, the Service Provider Discovery phase will return a single record; therefore, in such a deployment, the subscriber would not select the service provider and the initial response to Service Provider discovery could return the address of the Service Discovery functional entity.

6.2.2.2 IPTV Service Discovery and Service Access for Residential networks with IG

6.2.2.2.1 High Level Step 4a - IPTV Service Provider Discovery

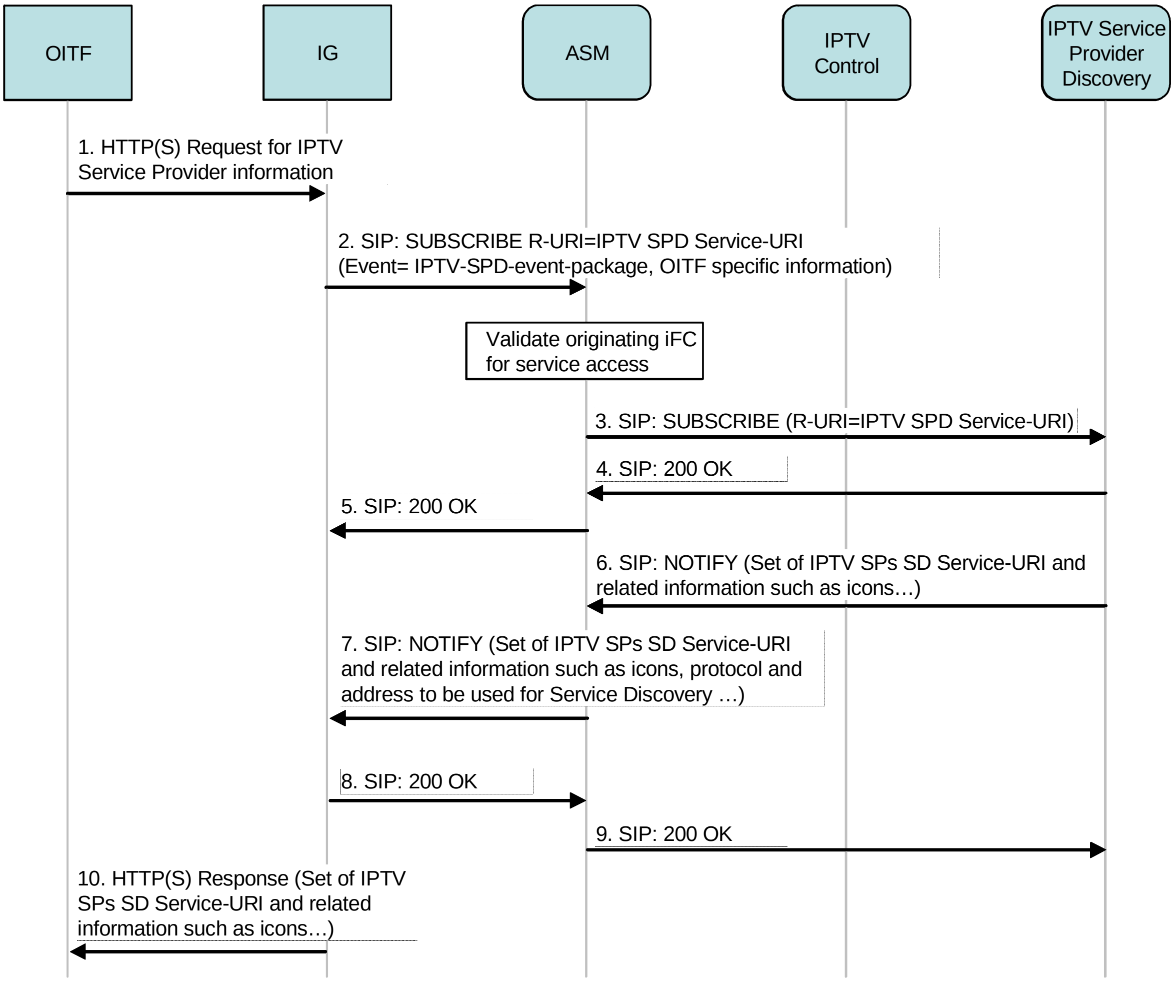

OITF
IG
ASM
IPTV Control
IPTV Service Provider Discovery
1. HTTP(S) Request for IPTV Service Provider information
2. SIP: SUBSCRIBE R-URI=IPTV SPD Service-URI (Event= IPTV-SPD-event-package, OITF specific information)
Validate originating iFC for service access
3. SIP: SUBSCRIBE (R-URI=IPTV SPD Service-URI)
4. SIP: 200 OK
5. SIP: 200 OK
6. SIP: NOTIFY (Set of IPTV SPs SD Service-URI and related information such as icons…)
7. SIP: NOTIFY (Set of IPTV SPs SD Service-URI and related information such as icons, protocol and address to be used for Service Discovery …)
8. SIP: 200 OK
9. SIP: 200 OK
10. HTTP(S) Response (Set of IPTV SPs SD Service-URI and related information such as icons…)

Figure 6-7: IPTV Service Provider Discovery for a managed network

The call flow in Figure 6-7 shows the case where the OITF requests, via the IG and the ASM, information about the available IPTV Service Providers from the Service Provider Discovery FE

Assumptions for this signal flow are that:

- The IG is registered with the SPP.
- The SPP has configured the IG.
- The IG knows the service URI of the IPTV Service Provider Discovery FE. This FE's service URI as well as the protocol to use to access it may be well known within the SPP domain.

In signals 2-7 the IG obtains a list of IPTV Service Providers available via the SPP. The result of this phase (step 10) is the retrieval of the list of IPTV Service Providers and related information (e.g. the IPTV Service Providers' name, IPTV SPs SD Service-URI (address of IPTV Service Discovery entity), protocol to be used for Service Discovery).

It is recommended that a well known Public Service Identifier (PSI) is assigned for the IPTV Service Provider Discovery functional entity. This well known PSI, which is a SIP URI, simplifies the remote configuration of IGs and allows IMS routing to be fully exploited.

The User Database is configured with the originating filter criteria necessary to route the SIP SUBSCRIBE messages from authorized users to the correct FE. In order to ensure that unauthorized users do not get access to the Service Provider Discovery FE, the PSI should not be configured in the DNS of the Service Platform Provider.

HTTP can optionally be used in this signal flow.

6.2.2.2.2 High Level Step 4b: IPTV Service Discovery

This procedure can be performed via the use of HTTP (case 1), or IGMP/multicast (case 2), depending on the “protocol to be used for Service Discovery” info obtained in High Level step 4a (see Figure 6-7).

IPTV Service Discovery – Case 1 – Using HTTP

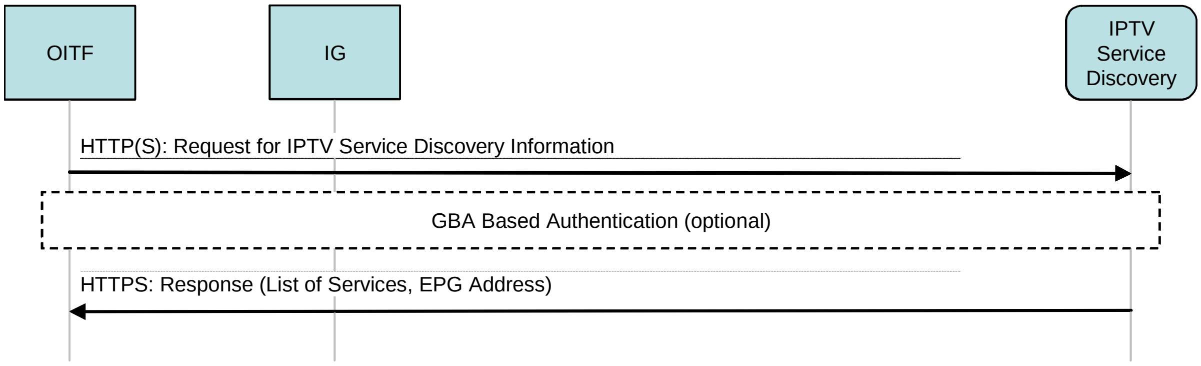

OITF
IG
IPTV Service Discovery
HTTP(S): Request for IPTV Service Discovery Information
GBA Based Authentication (optional)
HTTPS: Response (List of Services, EPG Address)

Figure 6-8: HTTP-based IPTV Service Discovery

The IPTV Service Discovery address is obtained in the high level step 4a shown in Figure 6-6.

In the flow shown in Figure 6-8, the OITF receives the address from where it can obtain the Content Guide as well the protocol to be used (via multicast or unicast).

The Service Discovery Record can be delivered to the OITF as XML data (for the metadata client) or a Web Page (for the DAE).

IPTV Service Discovery – Case 2 – Using IGMP multicast

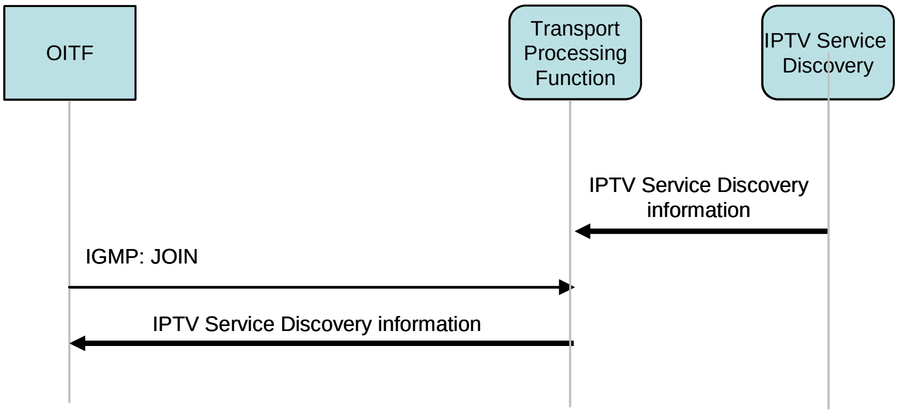

OITF
Transport Processing Function
IPTV Service Discovery
IPTV Service Discovery information
IGMP: JOIN
IPTV Service Discovery information

Figure 6-9: Multicast-based IPTV Service Discovery

The IPTV Service Discovery multicast address is obtained in the high level step 4a shown in Figure 6-6.

In the flow shown in Figure 6-9, the OITF joins the appropriate address using IGMP to obtain the IPTV service discovery information as XML data (for the metadata client).

6.2.2.2.3 High Level Step 5 - IPTV Service Access - Obtaining the Content Guide

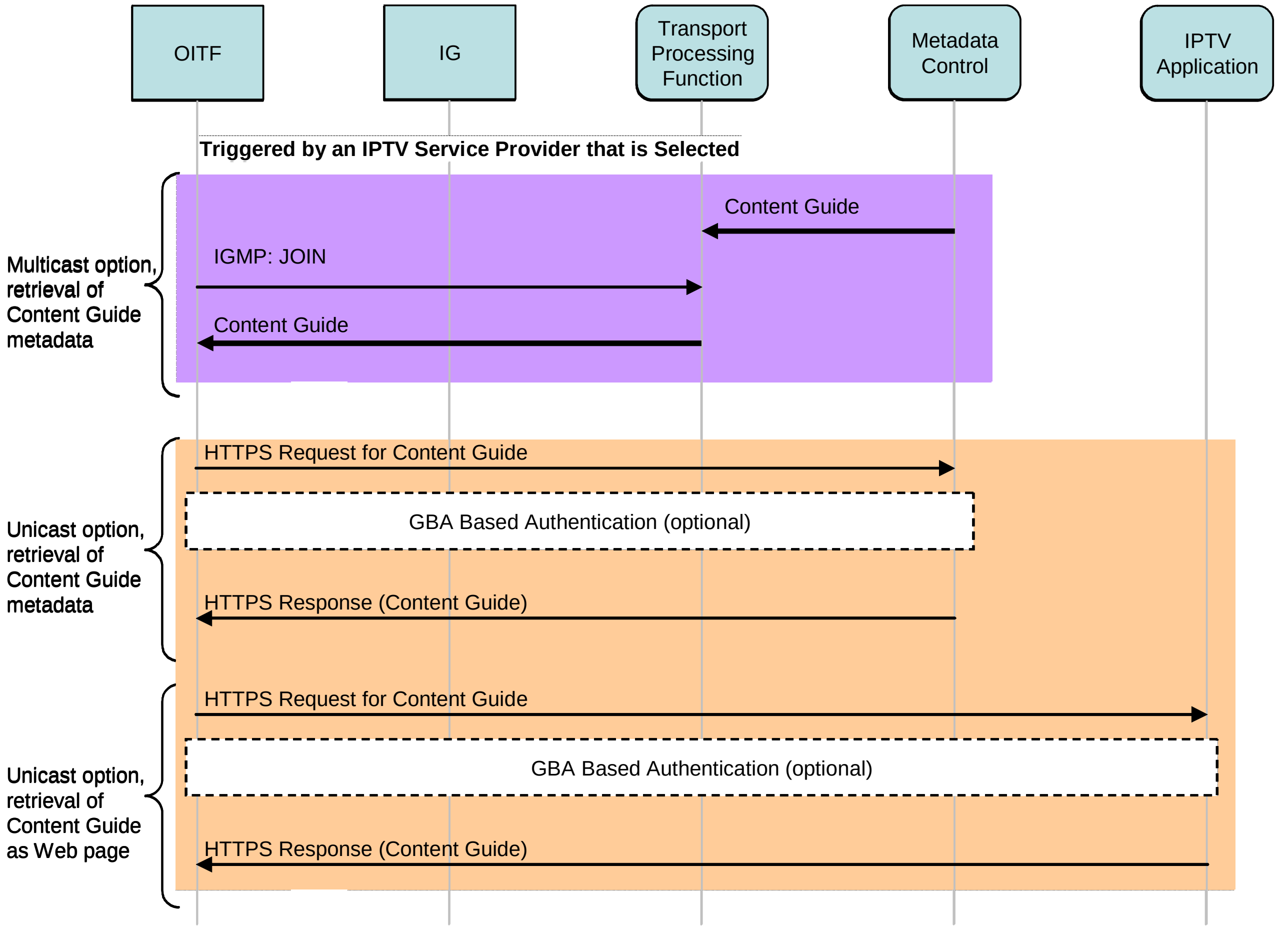

OITF
IG
Transport Processing Function
Metadata Control
IPTV Application
Triggered by an IPTV Service Provider that is Selected
Multicast option, retrieval of Content Guide metadata
Content Guide
IGMP: JOIN
Content Guide
Unicast option, retrieval of Content Guide metadata
HTTPS Request for Content Guide
GBA Based Authentication (optional)
HTTPS Response (Content Guide)
Unicast option, retrieval of Content Guide as Web page
HTTPS Request for Content Guide
GBA Based Authentication (optional)
HTTPS Response (Content Guide)

Figure 6-10: Access to Content Guide

Three possible flows are shown in Figure 6-10:

- Metadata based Content Guide delivered via multicast.
- Metadata based Content Guide delivered via unicast.
- Content Guide delivered via unicast in data formats supported by the DAE (e.g., HTML Web Page).

6.2.2.3 IPTV Service Discovery and Service Access for Residential Networks with IG and AG

6.2.2.3.1 High Level Step 4a - IPTV Service Provider Discovery

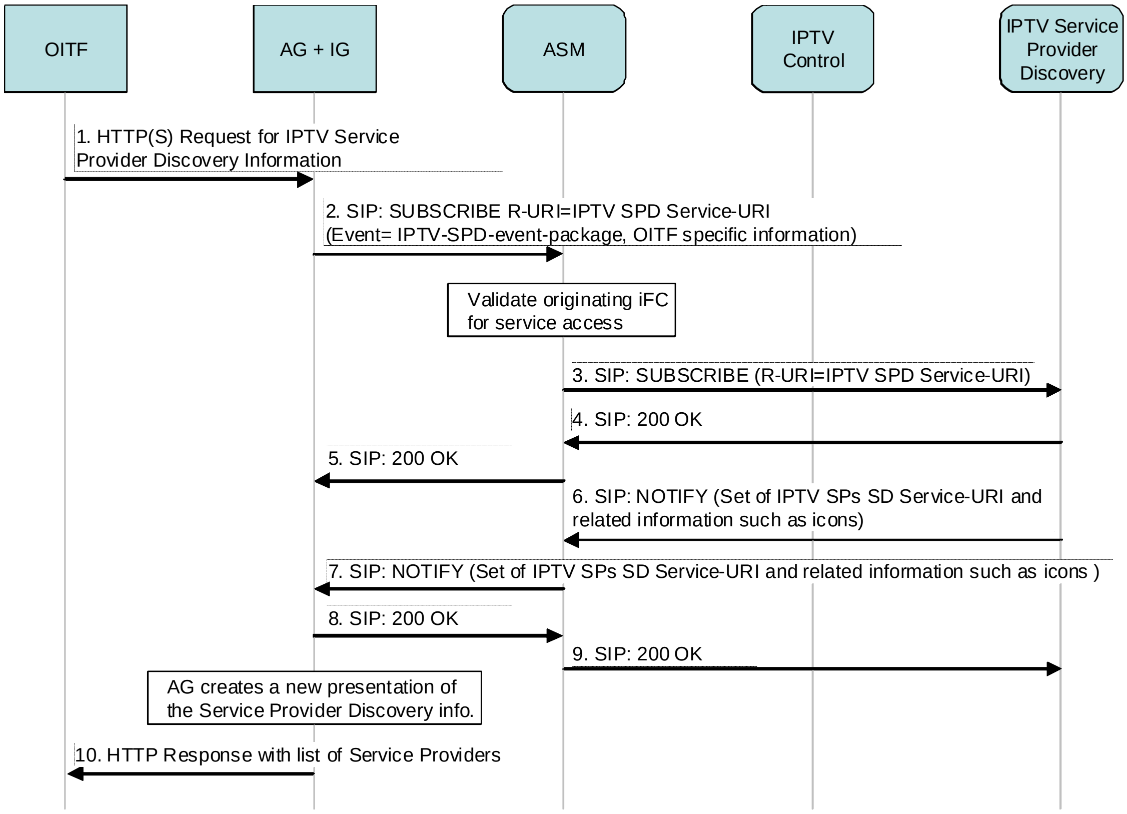

OITF
AG + IG
ASM
IPTV Control
IPTV Service Provider Discovery
1. HTTP(S) Request for IPTV Service Provider Discovery Information
2. SIP: SUBSCRIBE R-URI=IPTV SPD Service-URI (Event= IPTV-SPD-event-package, OITF specific information)
Validate originating iFC for service access
3. SIP: SUBSCRIBE (R-URI=IPTV SPD Service-URI)
4. SIP: 200 OK
5. SIP: 200 OK
6. SIP: NOTIFY (Set of IPTV SPs SD Service-URI and related information such as icons)
7. SIP: NOTIFY (Set of IPTV SPs SD Service-URI and related information such as icons)
8. SIP: 200 OK
9. SIP: 200 OK
AG creates a new presentation of the Service Provider Discovery info.
10. HTTP Response with list of Service Providers

Figure 6-11: Steps in Service Provider Discovery for a residential network with an AG and IG

The call flow in Figure 6-11 is very similar to the IG-only case. The only difference is that the AG intercepts the data, generates a web page and sends its address (URL) to the OITF for retrieval.

The assumptions for this signal flow are that:

- The IG is registered with the SPP.
- The SPP has configured the AG+IG.
- The AG+IG knows the Service-URI of the IPTV Service Provider Discovery FE. This FE's service-URI as well as the protocol to use to access it may be well known within the SPP domain.

In signals 2-7, the AG+IG obtains a list of IPTV Service Providers available at the SPP and converts this information into a suitable format, among those supported by the DAE. This conversion can be required, for example, to change the look & feel of the page listing the Service Providers**.**

Note that Service Provider Discovery info can be delivered as XML data (for the metadata client) or data formats supported by the DAE (e.g., HTML web page).

Analogous to the case where only the IG is deployed, it is recommended that a well known Public Service Identifier (PSI) is assigned for the IPTV Service Provider Discovery functional entity.. This well known PSI, which is a SIP URI, simplifies the remote configuration of IGs, and allows IMS routing to be fully exploited.

The User Database is configured with the originating filter criteria necessary to route the SIP SUBSCRIBE messages from authorized users to the correct FE. In order to ensure that unauthorized users do not get access to the Service Provider Discovery FE, the PSI is should not be configured in the DNS of the Service Platform Provider.

HTTP can be optionally be used in this signal flow.

6.2.2.3.2 High Level - Step 4b – IPTV Service Discovery

This procedure can be performed via the use of the IMS either HTTP, or IGMP/multicast, depending on the "protocol to be used for Service Discovery" information obtained in step 4a of the high level procedures (see Figure 6-7). For the sake of simplicity, no call flows are shown here as the other cases are very similar to those described in Section 6.2.2.2.2.

6.2.2.3.3 High Level Step 5 – IPTV Service Access

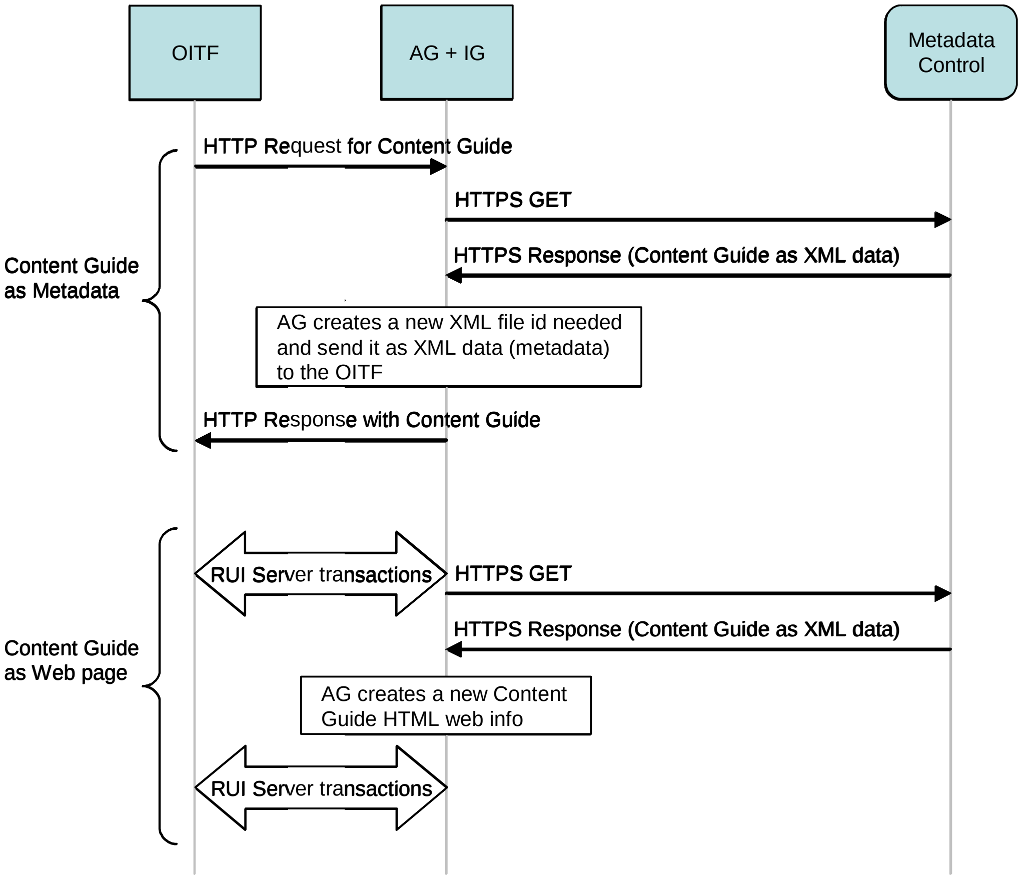

OITF
AG + IG
Metadata Control
HTTP Request for Content Guide
HTTPS GET
HTTPS Response (Content Guide as XML data)
Content Guide as Metadata
AG creates a new XML file id needed and send it as XML data (metadata) to the OITF
HTTP Response with Content Guide
RUI Server transactions
HTTPS GET
HTTPS Response (Content Guide as XML data)
Content Guide as Web page
AG creates a new Content Guide HTML web info
RUI Server transactions

Figure 6-12: Steps for Service Access in a residential network with an AG and an IG

Figure 6-12 shows XML data for creating the Content Guide (CG) being retrieved using HTTP.

6.2.3 Consolidated service discovery of managed and unmanaged services

For an OITF connected to a managed network, the OITF may present a consolidated view of the services discovered from the managed network, and also whatever is available from the default service discovery mechanisms for unmanaged network based SPs. At this point, if the user is allowed to enter preferences regarding the first screen, this will be seen when the OITF is powered on the next time.

6.3 User Identification and Authentication

For IPTV services that require service access authorization, the user is identified and authenticated by means of some pre-established credentials (such as user name and password, or IMS Private Identity [Ref 15] and corresponding long-term secret key). This section provides high-level message flows for user identification and authentication – for the case of unmanaged as well as managed networks.

For managed networks, the following user authentication methods shall be supported: IMS AKA and SIP Digest [Ref 18]. . HTTP Digest (RFC 2617) [Ref 16] shall be supported for the case of the unmanaged network model.

For Single Sign-on, 3GPP's Generic Bootstrapping Architecture (GBA) (3GPP TS 33.220) [Ref 25] shall be supported for managed networks, and SSL/TLS shall be supported for unmanaged networks. The Single Sign-on mechanisms provided by the Generic Bootstrapping Architecture may also be applicable for the unmanaged network model when UICC-based IMS authentication capability is available in the home.

6.3.1 Unmanaged Networks

For unmanaged networks, the solution should use HTTP Digest Authentication [RFC 2617] [Ref 16] in order to identify and authorize users for IPTV service access. The HTTP Digest Authentication scheme improves the HTTP Basic Authentication method by transmitting cryptographic hashes of passwords and other relevant data instead of transferring passwords from clients to servers as clear text. Figure 6-13 depicts the call flow for HTTP Digest Authentication between the relevant functional entities.

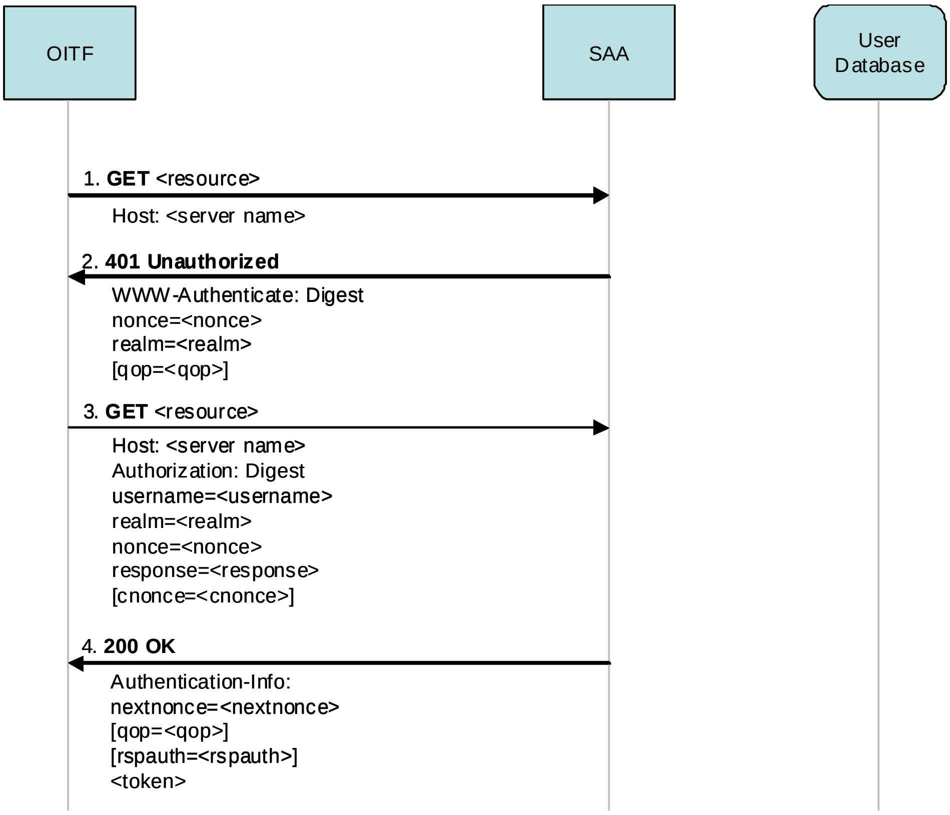


Figure 6-13: Identification and Authentication using HTTP Digest in the case of unmanaged networks

The following is a description of the various messages:

1. **OITF to SAA: HTTP GET**
   The OITF sends an HTTP GET request to the Service Access Authentication (SAA) function. This request

indicates the resource desired by the OITF (e.g., <resource> = /supercoolvideos.html) and the name of the server hosting the desired resource (e.g., <server name> = www.coolvideos.com).

2. **SAA to OITF: HTTP 401 Unauthorized**
Since access to the requested resource is protected, the SAA sends an HTTP 401 Unauthorized response to the OITF. This message contains a WWW-Authenticate header field which indicates that the OITF has to authenticate using the HTTP Digest method. To this end, this response message also includes a random value called nonce and the realm to which the requested resource belongs (e.g., <realm> = supercoolvideos@coolvideos.com). The Quality of Protection (qop) parameter is optional but if included by the HTTP Server, not only the OITF can be authenticated by the SAA but also vice versa (see step 3 and 4).

3. **OITF to SAA: HTTP GET**
The OITF resends the HTTP GET request to SAA, this time also including an Authorization header field in order to get authenticated by SAA. This header fields contains a user name valid for the realm in question and the response digest that the OITF has calculated based on input of the user name, corresponding password, realm and other data. If the HTTP 401 message in step 2 contained a qop parameter, the OITF challenges the SAA function for authentication by including a client nonce (cnonce). On reception of this HTTP GET message, the SAA compares the response value received from the OITF to the expected response value. (The SAA function obtains, at least partly, this expected response value from the User Database. The interface between the HTTP Server (SAA) and the User Database is out of scope of the Open IPTV Forum specifications.)

4. **SAA to OITF: HTTP 200 OK**
If the response value received from the OITF equals the expected response value (successful case), the SAA sends an HTTP 200 OK response to the OITF containing Authentication-Info header. The OITF can later on use the information in this header to send the HTTP GET request with an Authorization header including this value to authenticate the OITF and gain IPTV service access. In case the SAA included a qop parameter in message 2, this HTTP 200 OK message also contains a response auth digest value (rspauth) calculated using the cnonce value sent to the SAA in step 3. This rspauth value enables the OITF to authenticate the SAA.

6.3.2 Managed Networks

In the managed network case, user identification and authentication is based on either the 3GPP IMS Authentication and Key Agreement (AKA) or on SIP Digest [Ref 18] .

User authentication occurs during IMS Registration, which occurs either when:

a. The IG is powered up

or

b. The end user explicitly logs on for personalized services

6.3.2.1 IMS AKA

To support IMS AKA, a UICC with an ISIM or USIM application must be integrated into the IMS Gateway (IG). From the IMS point of view, the IG thereby takes the role of an IMS Subscriber. The UICC stores a long-term secret key K which is shared between the ISIM or USIM application and a User Database belonging to the network operator that provides the ISIM or the USIM. The following figure shows the high-level message flows for user identification and authentication based on the IMS AKA procedure:

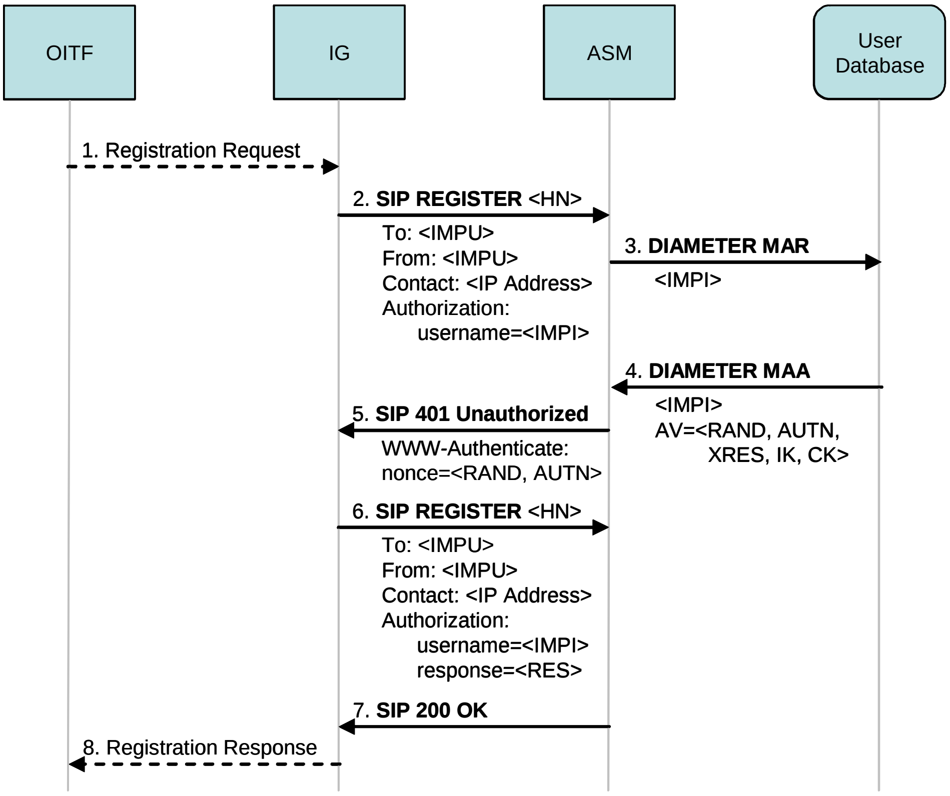


Figure 6-14: Identification and Authentication using IMS AKA in the managed case

The following is a description of the message flows shown in Figure 6-14:

1. **OITF to IG: Registration Request**
   The OITF sends a request for registration to the IMS Gateway (IG), when needed (case b. The end user explicitly logs on for personalized services)

2. **IG to ASM: SIP REGISTER**
   This request contains the domain name <HN> of the Residential network as read from the ISIM, the private and public IMS identities <IMPI> and <IMPU> of the IG, as well as IG's IP address (obtained prior to IMS AKA). Besides the IP address, all these data are read from the ISIM.

3. **ASM to User Database: DIAMETER MULTIMEDIA AUTH REQUEST (MAR)**
   ASM requests authentication data from the User Database with respect to the IMS subscriber (IG) identified by <IMPI>.

4. **User Database to ASM: DIAMETER MULTIMEDIA AUTH ANSWER (MAA)**
   The User Database sends an Authentication Vectors (AV) to the ASM containing the following data: random challenge RAND, answer XRES expected by the IG in step 6, network authentication token AUTN, integrity key IK, and ciphering key CK. The authentication token AUTN contains a message authentication code (MAC) enabling the IG to authenticate the HN (see step 8).

5. **ASM to IG: SIP 401 Unauthorized**
   At this point in time, the ASM denies the IG authentication. Instead, it sends a SIP Unauthorized message with a WWW-Authenticate header to the IG. This header contains RAND and AUTN. After reception of this message, the IG verifies the message authentication code contained in AUTN thereby authenticating its Residential network.

6. **IG to ASM: SIP REGISTER**
   ISIM computes the value RES on input of its version of the secret key K stored on the UICC of the IG. The IG sends a new SIP REGISTER request to the ASM, this time with RES as response to the challenge the ASM initiated in step 5.

7. **ASM to IG: SIP 200 OK**
   If RES = XRES (successful case), ASM considers the IG as authenticated, and binds <IMPU> to the IP address <IP address>.

8. **IG to OITF: Registration Response**
   The IG informs the OITF about the result of the registration procedure. (when step 1 is needed)

In case of success, the ISIM of the IG is able, based on its knowledge of the secret key K and the authentication token AUTN, to calculate the same values of the integrity key IK and the ciphering key CK as those that the ASM received in step 4 from the User Database. The IG and the ASM use IK and CK to establish IPSec Security Associations for protecting SIP signalling messages over the IG – ASM reference point.

6.3.2.2 SIP Digest

SIP Digest follows the 3GPP TS 24.229 specification [Ref 18].

6.3.3 Usage for GBA in the Unmanaged Model

In case where IMS-based authentication capability is supported and available in the home, the GBA Single Sign-on procedure can be used when accessing IPTV Application Servers that trust these IMS-based user credentials for service access. The unmanaged model shall use the same mechanism deployed in the managed model with regard to the usage of GBA. This applies in both the residential network and the SPP network.

6.4 Unicast Session

There are a number of IPTV services that use unicast delivery for all or part of their content delivery, such as:

- CoD, Content on Demand: End users can order videos through a CoD catalogue and have them streamed directly to the ITF
- nPVR, Network based Personal Video Recorder: Allows recording of programs on the network side, and delivered as a unicast stream when played back.
- Time Shifting: This allows the end user to pause, rewind and fast forward to the current position a live broadcast program. At the pause request, the network starts recording the session so that subsequent user actions (e.g., play, rewind) results in a unicast nPVR session.

6.4.1 Unicast Session setup (managed model)

Figure 6-15 shows a high level call flow for a unicast session setup based on the above descriptions. The unicast session setup procedure includes the following three call flows:

- Service Session setup.
- Secure Channel setup for the Content Delivery Session (optional).
- Content Delivery and Control.

Each of the above call flows will be described in separate sub-sections.

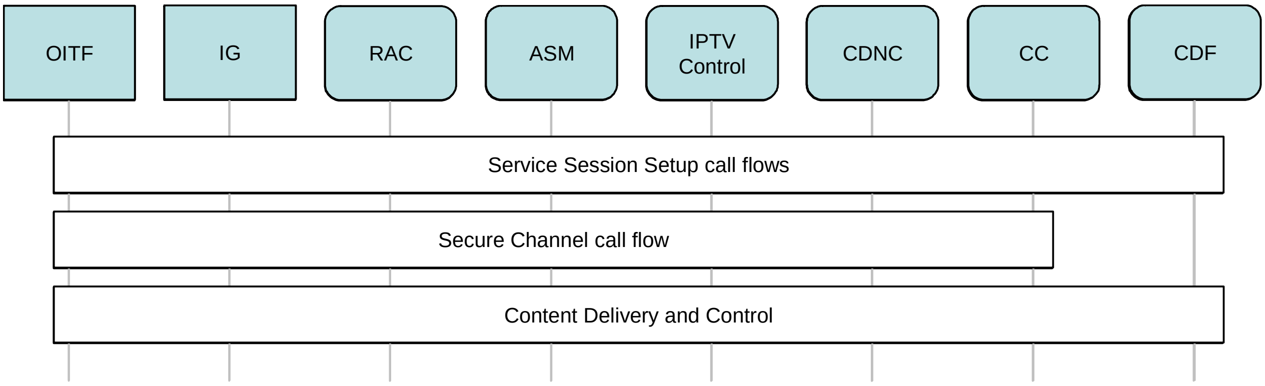
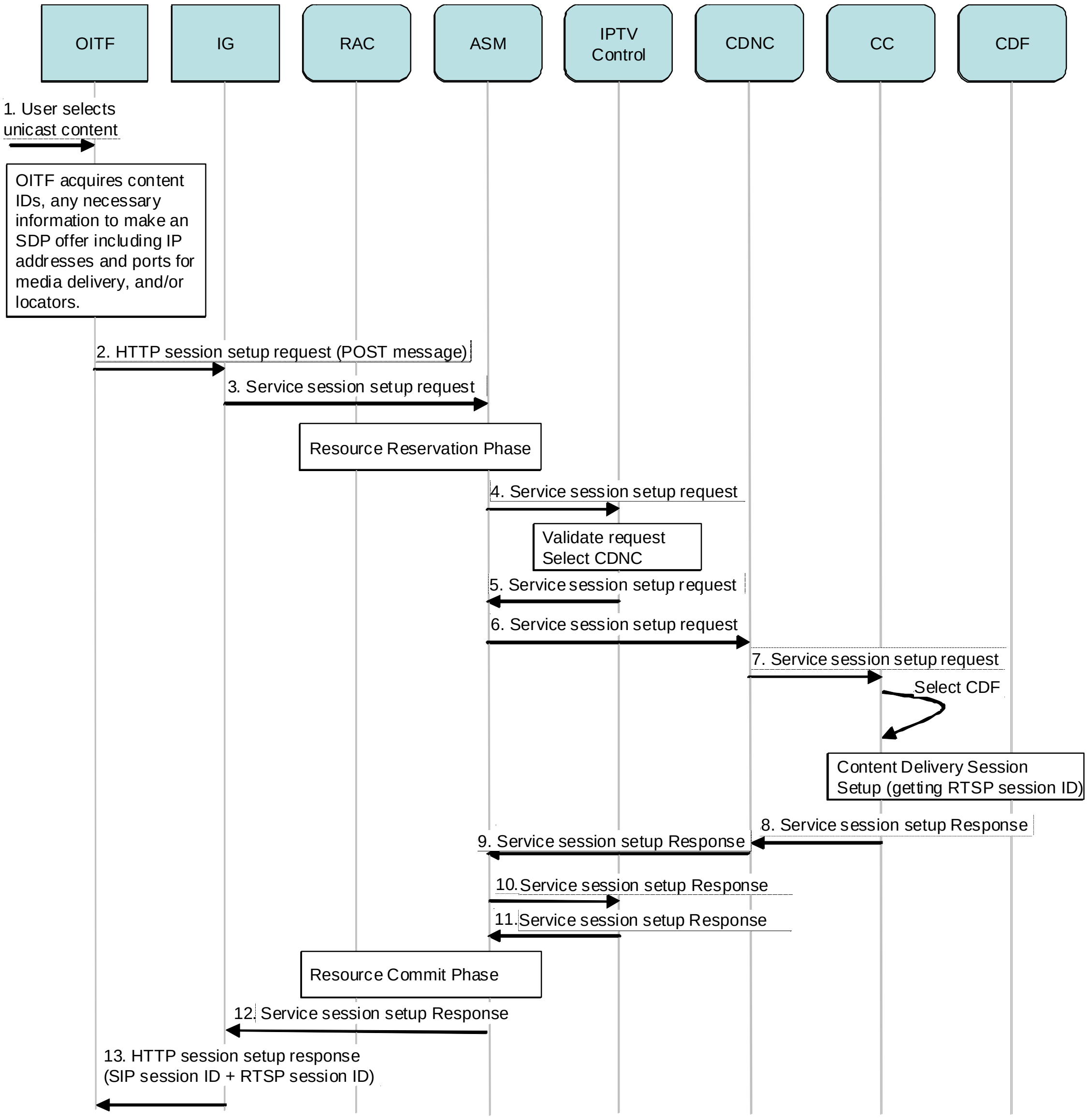

OITF
IG
RAC
ASM
IPTV Control
CDNC
CC
CDF
Service Session Setup call flows
Secure Channel call flow
Content Delivery and Control

Figure 6-15: Overall Description of the call flows

6.4.1.1 Service Session Setup Description

The Service Session establishment in the managed network model involves the OITF, the IG, the IPTV Control, the CDNC, the "Authentication and Session Management (ASM)" and the "Resource and Admission Control (RAC)" functional entities.



OITF
IG
RAC
ASM
IPTV Control
CDNC
CC
CDF
1. User selects unicast content
OITF acquires content IDs, any necessary information to make an SDP offer including IP addresses and ports for media delivery, and/or locators.
2. HTTP session setup request (POST message)
3. Service session setup request
Resource Reservation Phase
4. Service session setup request
Validate request Select CDNC
5. Service session setup request
6. Service session setup request
7. Service session setup request
Select CDF
Content Delivery Session Setup (getting RTSP session ID)
8. Service session setup Response
9. Service session setup Response
10. Service session setup Response
11. Service session setup Response
Resource Commit Phase
12. Service session setup Response
13. HTTP session setup response (SIP session ID + RTSP session ID)

Figure 6-16: Service Session Setup Call Flow

The following is a description of the interactions in the call flow shown in Figure 6-16:

1. The sequence is triggered by an action from the user. The user requests content from the CoD catalogue or selects some content stored in an nPVR, which results in a unicast session.

The OITF acquires all the necessary information about the selected content that allows it to make an SDP offer. The SDP offer must include the IP address and port of the OITF, which is the destination address of the stream for the selected content.

2. The OITF sends an HTTP session setup request to the IG. The request includes the selected content id and the corresponding SDP offer.

3. The IG sends a Service session setup request (SIP INVITE) to the ASM in the IMS core network.

The ASM uses the services of the “Resource and Admission Control” functional entity to perform resource reservation.

4. The ASM forwards the request to the IPTV Control functional entity.

The IPTV Control authorizes the request based on the user profile. The IPTV Control selects the appropriate CDN Controller. Optionally, the IPTV Control interacts with another functional entity that performs that task.

5. The IPTV Control forwards the request to the ASM for routing to the selected CDN Controller.

6. The ASM routes the request to the target Content Delivery Network Controller. The CDN Controller locates the appropriate Cluster Controller that can service the request.

7. The Content Delivery Network Controller forwards the Service session setup request to the chosen Cluster Controller

The Cluster Controller analyses the Service session setup request in order to choose the appropriate Content Delivery Function (CDF) based on its status, options and load (e.g. number of outgoing streams). Please refer to Annex C for more information about CDNC/CC/CDF selection.

The Cluster Controller then sets up the content delivery session (RTSP session) for the requested content, and establishes a binding between the service session and the corresponding content delivery session.

8-11. The content delivery session identification is returned, through the Service session setup response, back to the ASM.

The “Authentication and Session Management” FE instructs the “Resource and Admission Control” FE to commit the reserved resources.

12. The ASM forwards the Service session setup response to the IG

13. The IG sends an HTTP response to the OITF that includes the content delivery session identifier (RTSP session ID), and all relevant information to allow the OITF and the user to start viewing.

6.4.1.2 Securing Content Delivery Session Signalling (optional)

As shown in the HLA in Figure 5-2, a secure channel can be optionally established between the OITF and the Cluster Controller prior to any exchange of signalling messages. In particular, this allows the Cluster Controller and the OITF to mutually authenticate each other. This is particularly critical in environments where direct communication without such a secure authenticated channel is not desirable because of potential security risks.

Note that the secure channel can be torn down when there is no signalling to be exchanged between the OITF and the Cluster Controller. Thus, the secure channel can be set up on demand.

Figure 6-17 depicts the actual call flow over such a secure tunnel.

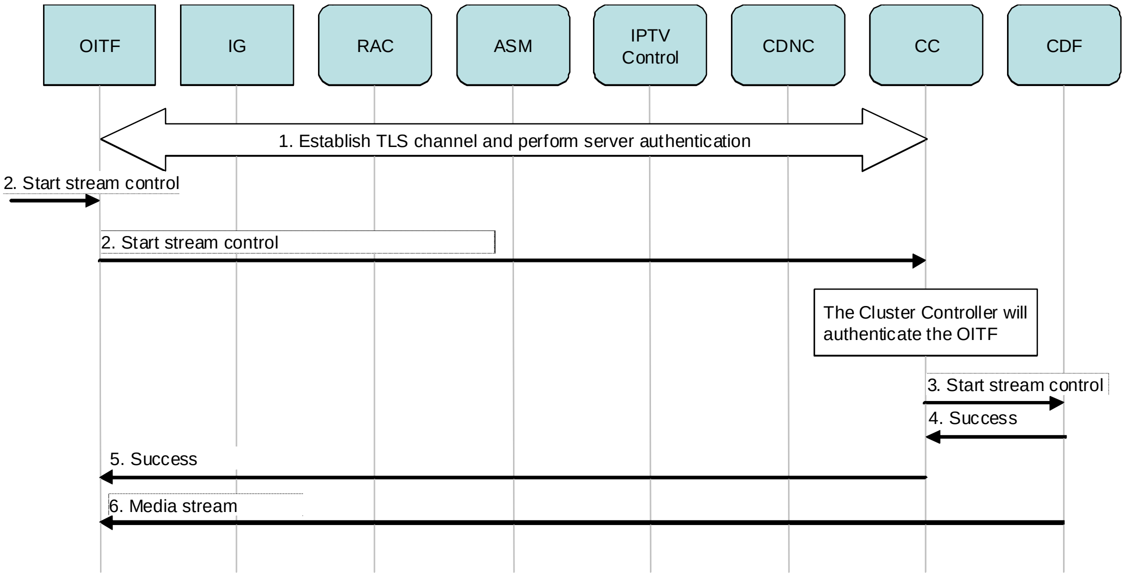


Figure 6-17: Securing the Content Delivery Signalling

The steps in this call flow are as follows.

1. The OITF establishes a TLS channel with the selected CC to serve the user. Server authentication is performed by the OITF in this step.
2. The OITF starts streaming control to start viewing the selected content.

The CC needs to authenticate the OITF before it proxies the message to the CDF.

3. Once mutual authentication is successfully completed, the CC proxies the start stream control message to the CDF.

4-5. The successful response from the Content Delivery functional entity is proxied all the way to the OITF.

6. Following that, the media streaming starts.

6.4.1.3 Content Delivery

After the service and content delivery sessions are setup, as explained in Section 6.4.1.1, the OITF uses the content delivery session ID to stream and control the content received from the CDF. A logical binding exists between the service session and the content delivery session. The binding is maintained by the CC, as well as the IPTV Control FE.

The steps in this call flow depicted in Figure 6-18 are as follows.

- Stream Control requests generated by the OITF are targeted to the CC. The CC proxies those requests to the appropriate Content Delivery Function.

- The Content Delivery Function streams the media directly to the OITF.

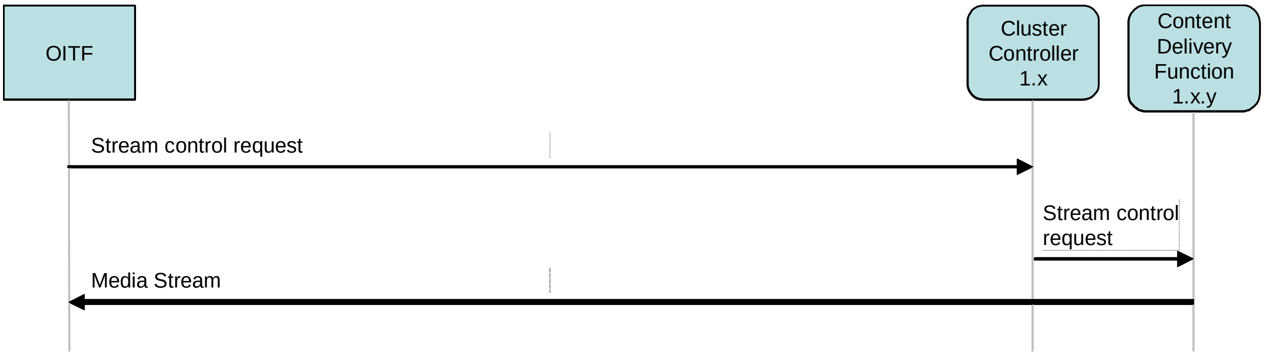


Figure 6-18: Content Delivery Streaming Control

6.4.2 Unicast Session Modification (managed network)

There are a number of use cases that can lead to the need for session modification. Examples include the need to receive a second stream for “picture-in-picture”, or simply to view a second channel in a side-by-side window with the original stream. These features depend on the capabilities of the rendering device. The implication of the above is that there can potentially be a 1:N relationship between a service session and the content delivery session.

Session modification can be initiated from the OITF or from the network side. The subsequent call flows show examples of both cases.

It is also important to note that modifying an existing session to include an additional stream is one option, while creating a new unicast session to carry that additional stream is another. Operator policies as well as client design can play a role here.

6.4.2.1 Client initiated session modification call flow

Figure 6-19 shows a typical call flow for the modification of an existing unicast session to add a new stream. Terminal capabilities must support such a feature in the first place.

It is assumed, that a Service Session and its associated Content Delivery Session(s) have been established prior to any modifications.

Below is a brief description of the steps that occur in this process:

1. The sequence is triggered by an action from the user. The user requests something from the CoD catalogue or selects some content stored in an nPVR. The user can optionally select a new Service Session to be setup for viewing that content or he can reuse an existing Service Session.

   The OITF acquires all the necessary information about the selected content that allows it to make to make an SDP offer. The SDP offer must include the IP address and port of the OITF, which is the destination address of the stream.

2. The OITF sends an HTTP session modify request to the IG. The request includes the selected content id, the corresponding SDP offer, and the service session id to be used for that session.

3. The IG sends a Service Modify request (SIP Re-INVITE) to the ASM in the IMS core network.

   The ASM uses the services of the “Resource and Admission Control” functional entity to perform resource reservation.

4. The ASM forwards the request to the IPTV Control functional entity.

   The IPTV Control FE authorizes the request based on the user profile. The IPTV control server selects the appropriate CDN controller. Optionally the IPTV control server interacts with another functional entity that performs that task.

5. The IPTV Control FE forwards the request to the ASM for routing to the selected CDN Controller.

6. The ASM routes the request to the target Content Delivery Network Controller. The CDN Controller locates the appropriate CC that can service the request.

7. The Content Delivery Network Controller forwards the Service modify request to the chosen Cluster Controller.

The Cluster Controller analyses the Service modify request in order to choose the appropriate Content Delivery Function based on its status, options and load (e.g. number of outgoing streams). Please refer to Appendix C more information about CDNC/CC/CDF selection.

The Cluster Controller then sets up the content delivery session (RTSP session) for the requested content, and establishes a binding between the Service Session and the corresponding Content Delivery Session.

8-11. The Content Delivery Session identification is returned, through the Service modify response, back to the ASM.

The “Authentication and Session Management” instructs the “Resource and Admission Control” to commit the reserved resources.

12. The ASM forwards the Service modify response to the IG.

13. The IG sends an HTTP response to the OITF that includes the Content Delivery Session identifier (RTSP session ID), and all relevant information to allow the OITF and the user to start viewing.

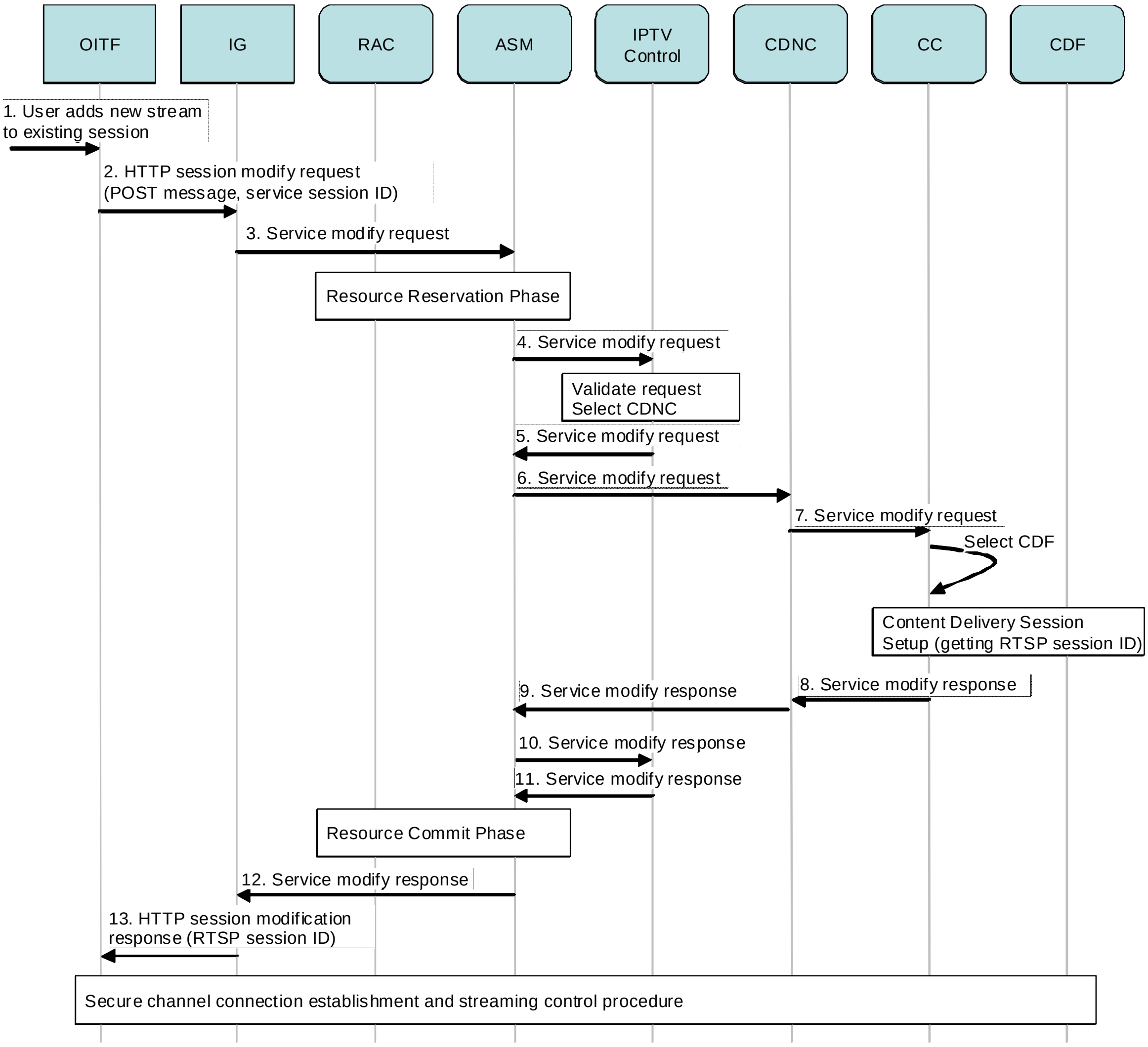

OITF
IG
RAC
ASM
IPTV Control
CDNC
CC
CDF
1. User adds new stream to existing session
2. HTTP session modify request (POST message, service session ID)
3. Service modify request
Resource Reservation Phase
4. Service modify request
Validate request
Select CDNC
5. Service modify request
6. Service modify request
7. Service modify request
Select CDF
Content Delivery Session Setup (getting RTSP session ID)
8. Service modify response
9. Service modify response
10. Service modify response
11. Service modify response
Resource Commit Phase
12. Service modify response
13. HTTP session modification response (RTSP session ID)
Secure channel connection establishment and streaming control procedure

Figure 6-19: OITF initiated Unicast Session Modification

6.4.2.2 Server Initiated Unicast Session

Figure 6-20 shows a typical call flow for a new unicast session generated from the network towards a registered user. Below is a brief description of the steps that occur in this process.

The sequence is triggered by an action from a network server. The server may have learnt somehow that a user is registered and decided to send an advertisement to the target user.

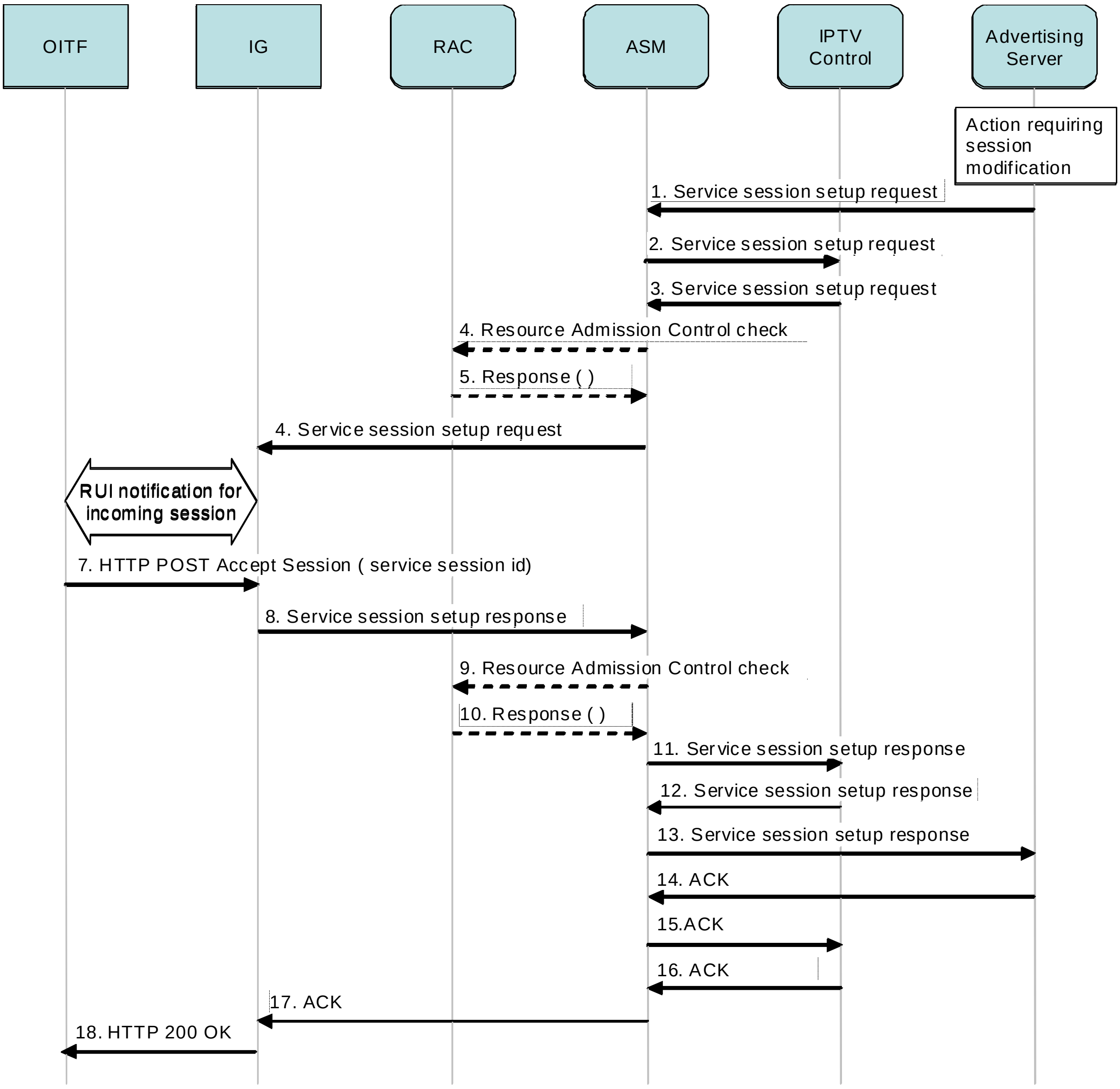

OITF
IG
RAC
ASM
IPTV Control
Advertising Server
Action requiring session modification
1. Service session setup request
2. Service session setup request
3. Service session setup request
4. Resource Admission Control check
5. Response ( )
4. Service session setup request
RUI notification for incoming session
7. HTTP POST Accept Session (service session id)
8. Service session setup response
9. Resource Admission Control check
10. Response ( )
11. Service session setup response
12. Service session setup response
13. Service session setup response
14. ACK
15.ACK
16. ACK
17. ACK
18. HTTP 200 OK

Figure 6-20: Network initiated unicast session modification

1. The advertising server (or any other network server) sends a Service session setup request to the Authentication and Session Management functional entity.

2. The Authentication and Session Management functional entity, based on the Subscription profile, forwards the request to the IPTV Control for further processing.

3. The IPTV Control has the option, based on operator policy, to either initiate a completely new session for the user or modify an existing unicast session for that user. The IPTV Control functional entity is always in the signalling path and retains state information for all ongoing unicast sessions. In this example, the IPTV Control functional entity decides to initiate a new unicast session for the target user. Hence, it initiates a Service session setup request to the ASM.

4-5. The Authentication and Session Management functional entity performs admission control for the new session. This step is optional for the managed model.

6. The ASM forwards the Service session setup request to the IG.

The IG performs the necessary RUI procedures to notify the OITF of an incoming session.

7. The OITF sends an HTTP POST to the IG to indicate its acceptance of the incoming session.

8. The IG sends a Service session setup response back to the ASM.

9-10. The ASM commits the reserved resources for the new session. This step is optional for a managed network.

11-13. The Service session setup response is forwarded all the way to the network server that initiated the session.

14-17. The network acknowledges the receipt of the response. This gets forwarded all the way to the IG.

18. The IG sends an HTTP response to the OITF.

6.4.3 Session Teardown (managed model)

Figure 6-21 shows a typical call flow for a unicast session tear down.

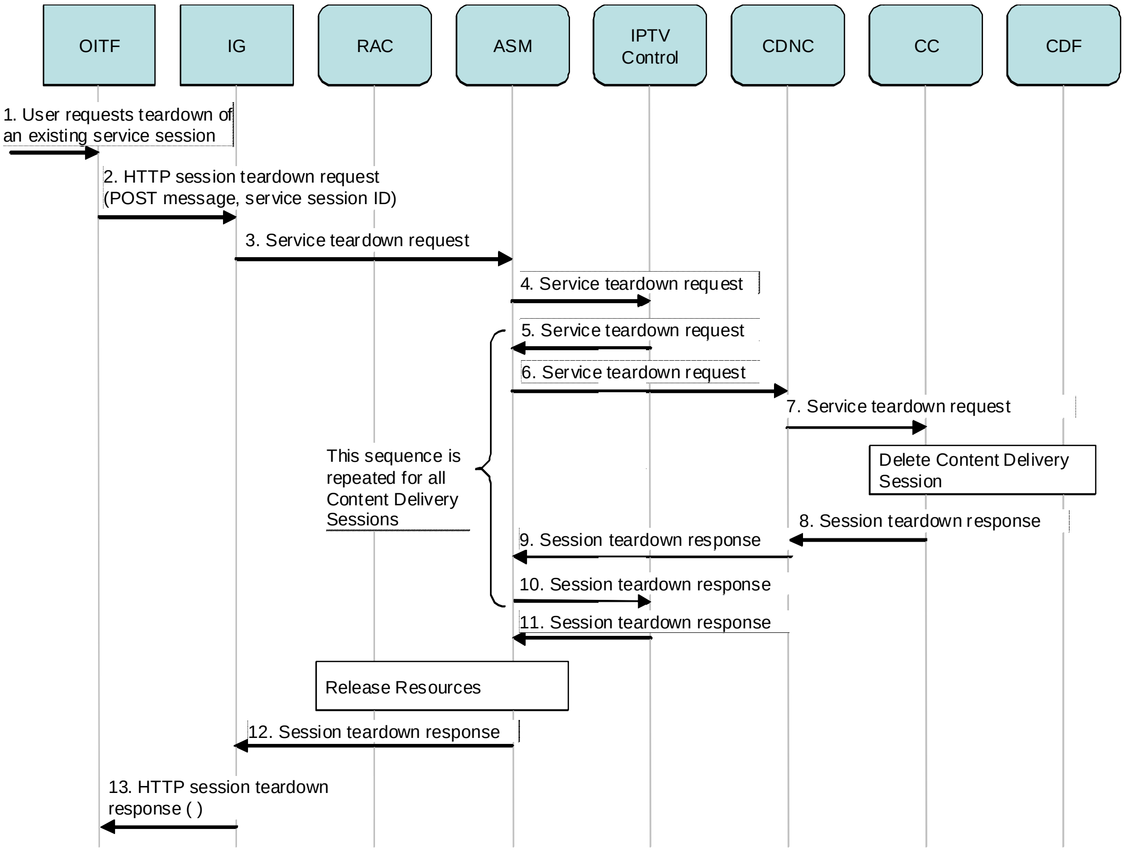

OITF
IG
RAC
ASM
IPTV Control
CDNC
CC
CDF
1. User requests teardown of an existing service session
2. HTTP session teardown request (POST message, service session ID)
3. Service teardown request
4. Service teardown request
5. Service teardown request
6. Service teardown request
7. Service teardown request
Delete Content Delivery Session
This sequence is repeated for all Content Delivery Sessions
8. Session teardown response
9. Session teardown response
10. Session teardown response
11. Session teardown response
Release Resources
12. Session teardown response
13. HTTP session teardown response ( )

Figure 6-21: Service Session tear down call flow

It is assumed that a Service Session and one or more associated Content Delivery sessions are ongoing before teardown can occur.

The following is a brief description of the steps that occur in this process:

The sequence is triggered by an action from the user, which results in the OITF requesting the termination of an ongoing unicast session which may or may not have an ongoing live stream.

1. The end user requests the termination of an ongoing unicast service session.

2. The OITF sends an HTTP teardown request to the IG. The request includes the service session id.

3. The IG sends a session tear down request to the Authentication and Session Management functional entity.

4. The request is forwarded to the IPTV Control functional entity.

5. The IPTV Control uses the Authentication & Session Management to route the request to the appropriate Custer Controller function that should be contacted to handle that request.

Note that steps 5-10 are repeated for each content delivery session associated with the service session.

6. The Authentication & Session Management functional entity forwards the request to the target CDNC functional entity.

7. The CDNC locates the appropriate CC.

The target Cluster Controller function locates the Content Delivery Function for the content delivery session, and sends a request to terminate the streaming session.

8. The Content Delivery Function responds successfully to the Session teardown request.

9-11. The Session teardown response is proxied all the way to the Authentication and Session Management functional entity.

The Authentication & Session Management functional entity requests the release of the resources allocated to the unicast session by communicating with the Resource and Admission Control functional entity.

12. The Authentication & Session Management functional entity forwards the Session teardown response to the IG.

13. The IG sends an HTTP response back to the OITF.

6.4.4 Unicast Session Management (unmanaged model)

Unicast session management for media streaming in an unmanaged network model differs from the managed network in that no resource management is performed in the network. This means there is no interactive management of the session – a new content delivery session is created for each unicast stream. This requires setup at the ITF and the content delivery function, but not in the network itself.

6.4.4.1 Access to Service Providers over unmanaged networks

This call flow is equivalent to the content guide retrieval described in Section 6.2.1.5.

6.4.4.2 Purchase of content from Service Providers over unmanaged networks

The call flow in Figure 6-22 shows the steps used to purchase service or content from an IPTV Service Provider accessed over an unmanaged network.

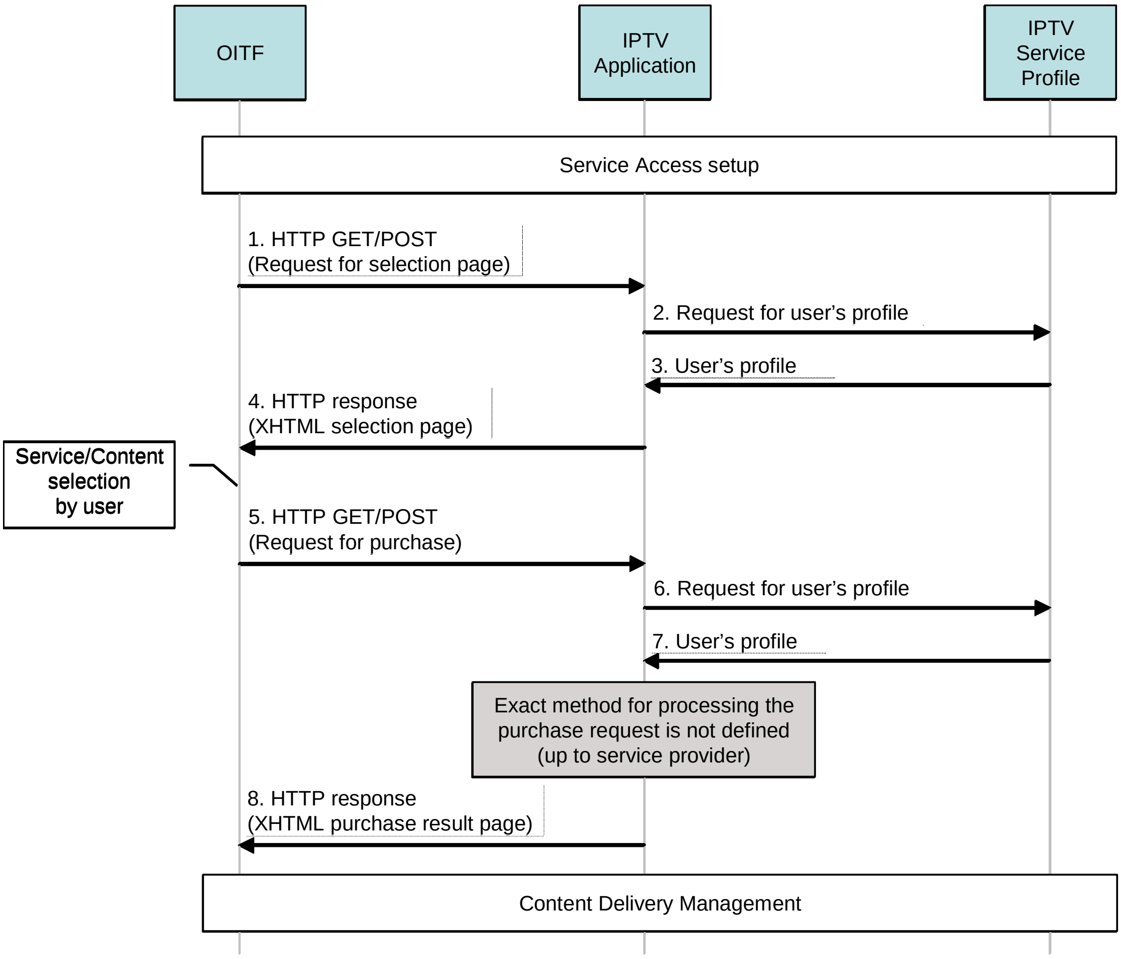

OITF
IPTV Application
IPTV Service Profile
Service Access setup
1. HTTP GET/POST (Request for selection page)
2. Request for user's profile
3. User's profile
4. HTTP response (XHTML selection page)
Service/Content selection by user
5. HTTP GET/POST (Request for purchase)
6. Request for user's profile
7. User's profile
Exact method for processing the purchase request is not defined (up to service provider)
8. HTTP response (XHTML purchase result page)
Content Delivery Management

Figure 6-22: Call flow for purchase of content from an IPTV Service Provider over unmanaged networks

The following is a brief description of the steps involved in the process.

1. Shows the OITF sending a HTTP GET or POST request to the IPTV Application, to acquire an XHTML page which contains the list of content. [Note: Signal 1 could be substituted by the request to the Metadata Control FE for XML based metadata, to be used by the Metadata-based CG client in the OITF for presentation of a Content Guide to the user].

2-3. Involves the IPTV Application retrieving the user profile from the IPTV Service Profile functional entity, to customize the HTML page according to the user's profile. These steps are optional.

4. Carries a response back to the OITF including the XHTML page which contains the list of content. [Note: Signal 4 could be substituted by the response carrying XML metadata from the Metadata Control FE, to be used by the Metadata-based CG client on OITF for presentation of a Content Guide to the user].

5. Shows the OITF sending a HTTP GET or POST request to the IPTV Application, to request the purchase of a specific service or content which the user has selected.

6-7. Shows the IPTV Application retrieving the user profile from the IPTV Service Profile function to process the purchase request based on data in the user's profile. These steps are optional.

8. Carries a response back to the OITF including the XHTML page which contains the result of the purchase request. The actual processing of the purchase request is done before this step, but the exact method is not defined (and is specific to the service provider). This page could also include links for the content acquisition, or an automatic redirection to the content acquisition function.

6.4.4.3 Unmanaged content delivery management

The call flow in Figure 6-23 shows the steps used to manage a unicast session in the case of an unmanaged network.

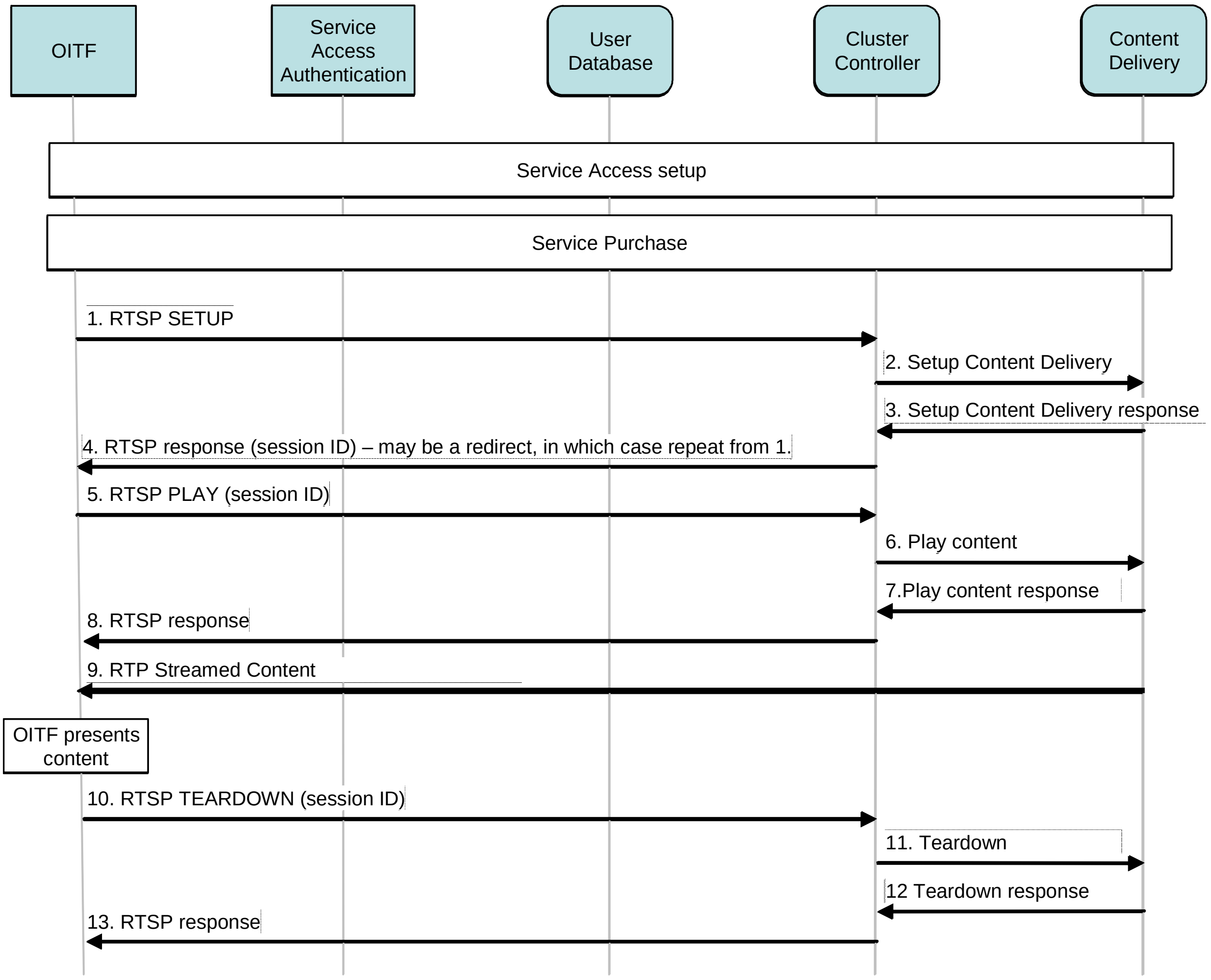


Figure 6-23: Call flow for unicast session management for an unmanaged network

The following is a brief description of the steps involved in a unicast content delivery session.

1. Shows the OITF sending a setup request to the Cluster Controller, to initiate a content delivery session, using a previously acquired SDP.

   Note: The SDP describing the requested media could be acquired from the content guide or using an RTSP DESCRIBE [Ref 19]. The exact method is left to the detailed protocol specifications.

2-3. Involves the Cluster Controller and the Content Delivery functions setting up the necessary resources for content delivery.

4. Carries a response back to the OITF. If the request is successful, a session identifier will be returned by the Cluster Controller. Alternatively, the response may redirect the OITF to another Cluster Controller, for example for load balancing reasons. The exact mechanism for achieving this is left to the detailed protocol specifications. In this case, the OITF would repeat the process from signal 1 to re-issue the request to the specified Cluster Controller.

5. Requests the Cluster Controller function to start streaming the content to the OITF.

6-7. Sets up the start the streaming of the content from the Content Delivery function.

8. Returns the status to the OITF.

9. Represents the content being streaming from the Content Delivery functional entity to the OITF.

10. Occurs at some later time, when the OITF no longer wishes to receive the stream.

11-12. Completes the teardown process and signal 13 returns the result to the OITF.

Note: The detailed specifications shall consider methods to prevent DOS attacks on Cluster Controllers, and to prevent session ID hijacking.

6.5 Scheduled Content Session Management Procedures

Scheduled content (often referred to as linear TV) is a basic service offered by an IPTV Service Provider. It is associated with IP multicast delivery mechanisms in a managed network, since several users would typically be watching the same channel within the same vicinity, serviced by the same network access node. This allows for considerable bandwidth saving in the access and core network, as a single stream from the source is routed as close as possible to the network access node, and from there on individual streams can be replicated and sent to individual users that want to watch that stream.

Scheduled content service allows a user to watch and zap between channels. When a user zaps to view a new channel, the ITF joins a multicast group that is associated with that channel, while leaving the multicast group associated with the old channel to which the ITF is currently tuned.

In a managed network, it is important to ensure that:

- a user is allowed to join a multicast group only if there is enough bandwidth with the right service priority to handle the requested stream within the access network. Otherwise the service can result in a bad user experience and bad picture quality;
- the reserved subscriber resources (last mile) are released when conditions for such a release present themselves (the user stops watching scheduled content TV and switches to CoD, the TV is powered off, etc.);
- during channel zapping, interaction or handshake between network entities related to bandwidth, service priority or admission control are optimized. This saves precious time and contributes to a faster channel zapping speed.

6.5.1 Scheduled Content session set-up

Scheduled content session set-up procedures should be established at ITF power up, after successful authentication and identification and content guide retrieval.

Figure 6-24 shows a call flow for the scheduled content session set-up.

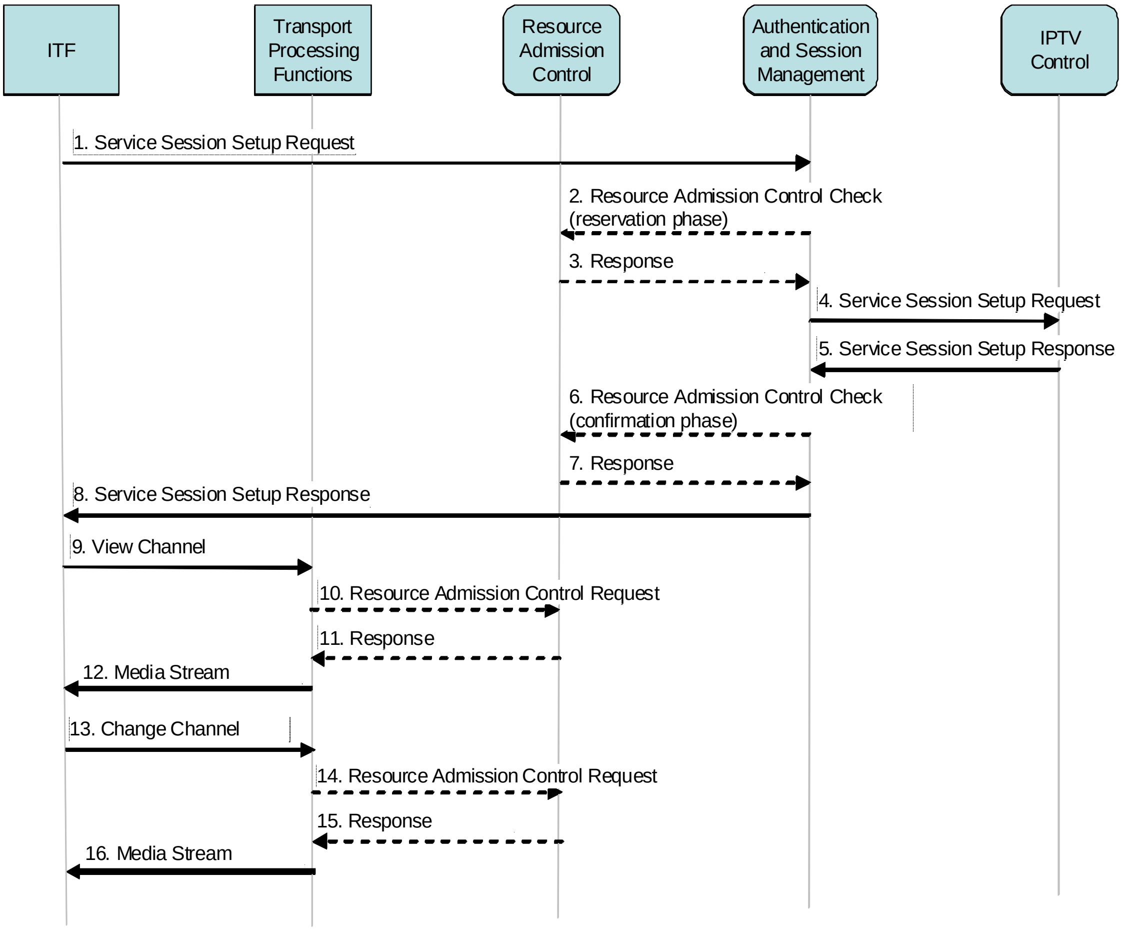

ITF
Transport Processing Functions
Resource Admission Control
Authentication and Session Management
IPTV Control
1. Service Session Setup Request
2. Resource Admission Control Check (reservation phase)
3. Response
4. Service Session Setup Request
5. Service Session Setup Response
6. Resource Admission Control Check (confirmation phase)
7. Response
8. Service Session Setup Response
9. View Channel
10. Resource Admission Control Request
11. Response
12. Media Stream
13. Change Channel
14. Resource Admission Control Request
15. Response
16. Media Stream

Figure 6-24: Call flow for scheduled content session setup

The following is a brief description of the steps in the flow:

1. The ITF sends a Service session setup request to the Authentication and Session Management FE, including a media offer for the scheduled content service

2. The Authentication and Session Management reserves transport resources according to the media offer

3. The response for the reservation request is returned.

4. The Authentication and Session Management FE forwards the request to the IPTV Control, which verifies that the user is authorized for the service and verifies that the user has the rights to consume the content.

5. The IPTV Control replies to the Authentication and Session Management with the bandwidth required for the specific scheduled content channels and may retrieve other parameters

6. (optional) If the media offer has changed or new parameters are received, the Authentication and Session Management requests admission control for the confirmation phase.

7. If step 6 is used, the response for the admission control request is returned.

8. Finally, the Service session setup response for the Service session setup request is forwarded to the ITF.

9. The ITF sends a request to the Transport Processing Functions to view the channel.

10,11. (optional) An interaction between the Transport Processing Functions and Resource Admission Control entities occurs in order to guarantee the needed bandwidth for the channel. This may happen in a number of cases, for example when the multicast channel is not present at network access node to which the user is connected, or when the ITF wishes to join a multicast channel with different QoS requirements (e.g. zapping from a SD to a HD channel),

12. Following that, the media stream is forwarded to ITF.

13. The ITF sends a request to the Transport Processing Functions to change the channel.

14-15. The operation is identical to that of step 10-11

16. Following that, the media stream is forwarded to ITF.

Appendix E gives a more detailed description of the Transport Processing Functions and the relation with Resource and Admission Control for an xDSL access network.

6.5.2 Scheduled Content service session teardown procedure

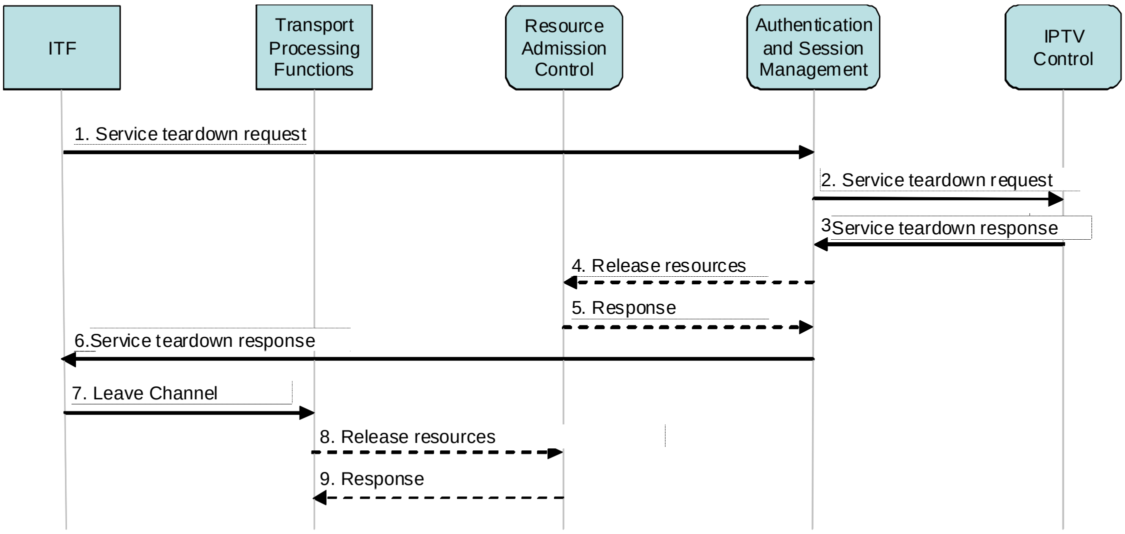

ITF
Transport Processing Functions
Resource Admission Control
Authentication and Session Management
IPTV Control
1. Service teardown request
2. Service teardown request
3Service teardown response
4. Release resources
5. Response
6.Service teardown response
7. Leave Channel
8. Release resources
9. Response

Figure 6-25: Scheduled Content service Session Teardown call flow

Figure 6-25 shows a typical call flow for tearing down a scheduled content session. The following is a brief description of the steps in the flow. The call flow assumes that a pre-condition for clearing a channel has occurred, such as the ITF being powered off, or the user switching to a CoD service, etc.

1. The ITF sends a Service teardown request to the Authentication & Session Management Functional Entity (FE).

2. The Authentication & Session Management Functional Entity forwards the request to the IPTV Control Functional Entity (FE).

3. The IPTV Control FE updates its internal states, if required, and sends a Service teardown response back to the Authentication & Session Management FE.

4. If resources have been reserved for the channel, the Authentication & Session Management FE reports the release to the Admission Control FE

5. The Admission Control FE responds back to acknowledge the release

6. The Session Management FE forwards the response to the ITF

7. The ITF sends a request to the Transport Processing Functions to stop streaming;

8,9. (optional) Internal to the Transport Processing FE, if the multicast channels are no longer needed at the access node for other users, the Transport Processing FE interacts with Admission Control to release the associated resources.

6.6 Push Content session management procedures (managed networks)

The Push procedure defines a mechanism for supporting IPTV Service Provider initiated IPTV services as, for example, Push CoD.

The content can be pushed to an OITF, asynchronously, during the period when the user is registered with the IMS domain. The Push Content session management procedure can potentially be used to deliver personalized content or other information to the OITF, in a personalized way, depending on user profile, user preferences or explicit interests.

The Push Content Session Management Procedure for the managed network can be based on a similar procedure already defined in other standards.

Figure 6-26 depicts an informational flow for the Push procedure, applied to the Push CoD service.

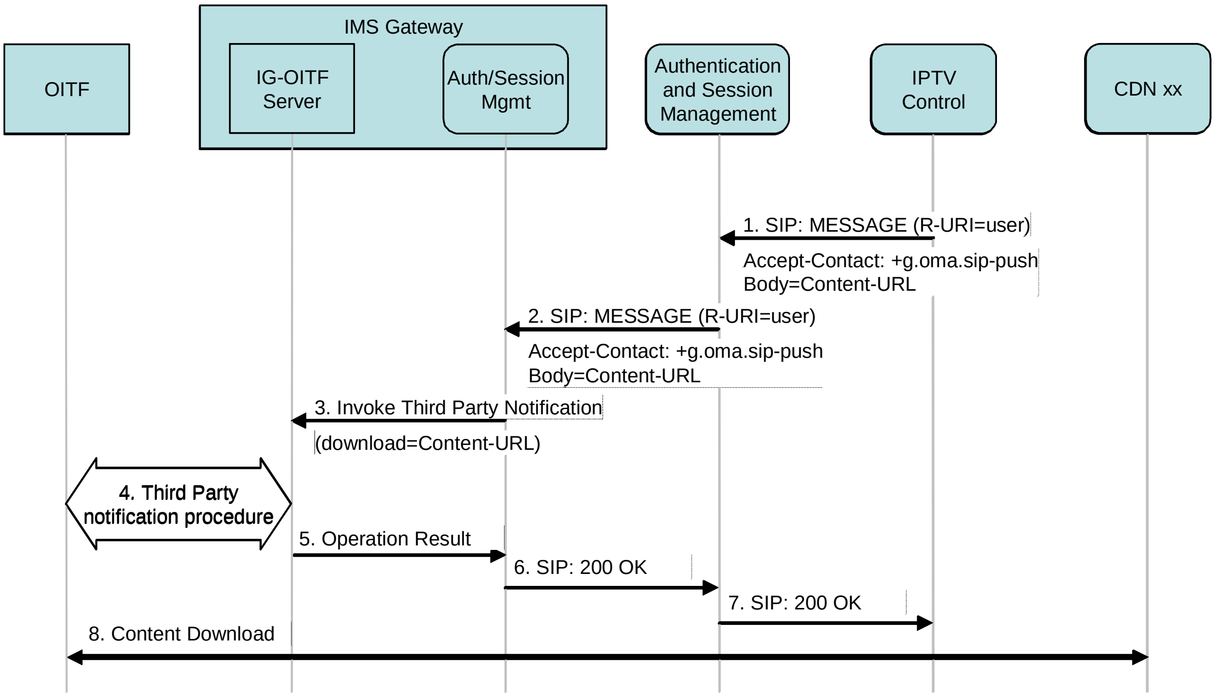

IMS Gateway
OITF
IG-OITF Server
Auth/Session Mgmt
Authentication and Session Management
IPTV Control
CDN xx
1. SIP: MESSAGE (R-URI=user)
Accept-Contact: +g.oma.sip-push
Body=Content-URL
2. SIP: MESSAGE (R-URI=user)
Accept-Contact: +g.oma.sip-push
Body=Content-URL
3. Invoke Third Party Notification
(download=Content-URL)
4. Third Party notification procedure
5. Operation Result
6. SIP: 200 OK
7. SIP: 200 OK
8. Content Download

Figure 6-26: Call flow for pushed content session management

The following is a brief description of the steps in the flow:

1. The IPTV Control sends a SIP MESSAGE to the Authentication and Session Management FE; the SIP MESSAGE includes:
   - In the *Accept-Contact* header a specific tag identifying that the MESSAGE is related to a Push procedure;
   - In the body, the *Content-URL* of the content to be downloaded by the OITF.
2. The SIP MESSAGE is sent to the user IMS Gateway where it is intercepted by the Authentication/Session Management function

3. The Authentication/Session Management function invokes the third party notification functionality in the IG-OITF Server function.

4. The IG-OITF Server function starts the notification procedure in the OITF using a DAE.

   Two possible solutions for the notification procedure are

   - "Third Party Notification Procedure": In this solution the IG-OITF-Server sends the appropriate CEA-2014 [Ref 3] operations so that the OITF can display the appropriate message. In more detail:
     - The IG-OITF Server creates locally the notification message (multicast) and sends it to the OITF. This message contains the reference/link to the "notification content".
     - The OITF receives the notification message and loads, from IG-OITF Server, the content referred to by the "notification content". In this case the "notification content" contains a scripting object (which includes the *Content-URI*) that triggers, on the OITF, the download of the content from the CDN.
     - The OITF sends the response to the IG-OITF Server after the "notification content" has loaded;
   - UPnP GENA [Ref 28]

5. The IG-OITF Server function reports the Operation Result to the Authentication/Session Management. function on the IMS Gateway;

6-7. The response to the SIP MESSAGE is forwarded to the IPTV Control via Authentication and Session Management;

8. The OITF executes the scripting object (received during the third party notification procedure [step 4]) and starts the downloading of the content from CDN. Note that the OITF UI client must have the "notificationscript" capabilities active.

6.7 User Profile Management

User profile management refers to the set of operations that allow a user to manage his profile. This includes the ability to create, fetch, modify, delete, or replace the profile.

Below is an example for a call flow to illustrate the roles played by different entities involved in user profile management

6.7.1 Profile Fetching - Unmanaged Model

This use case includes an end user fetching his profile, updating it and then uploading it. The call flow for this use case is shown in Figure 6-27.

The following is a brief description of the steps:

1. An end user, through the GUI, selects the profile fetching option.
2. The OITF sends an HTTP GET request to the IPTV Service Profile FE. The request includes the user identity.
3. The IPTV Service Profile FE authenticates the user identity.
4. The response is returned.
5. The IPTV Service Profile FE verifies the authorization policies associated with the profile against the identity in the incoming request and subsequently returns the profile to the OITF in a 200 OK.

The received profile is displayed to the user who performs the desired updates, and is ready now to upload the new profile.

6. The end user, through the GUI, selects the profile update option.
7. The OITF sends an HTTP PUT request to the IPTV Service Profile FE. The request includes the user identity.
8. The IPTV Service Profile FE authenticates the user identity.
9. The response is returned.
10. The IPTV Service Profile FE verifies the authorization policies associated with the profile against the identity in the incoming request and subsequently returns to the OITF a 200 OK after updating the profile.

The GUI displays to the user the received response.

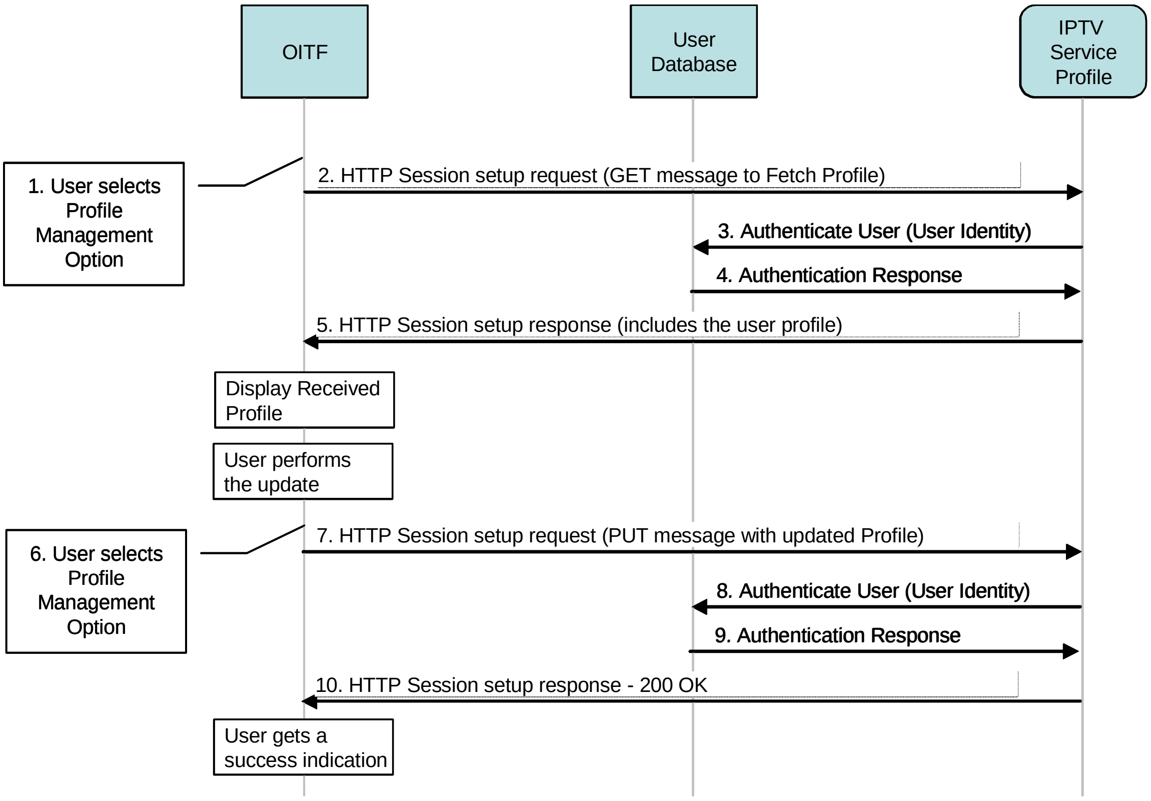

OITF
User Database
IPTV Service Profile
1. User selects Profile Management Option
2. HTTP Session setup request (GET message to Fetch Profile)
3. Authenticate User (User Identity)
4. Authentication Response
5. HTTP Session setup response (includes the user profile)
Display Received Profile
User performs the update
6. User selects Profile Management Option
7. HTTP Session setup request (PUT message with updated Profile)
8. Authenticate User (User Identity)
9. Authentication Response
10. HTTP Session setup response - 200 OK
User gets a success indication

Figure 6-27: Profile fetching, and update in the Unmanaged Model

6.8 Parental Control for CoD

An example of parental control within the context of CoD services, and using communication services, refers to the ability of the IPTV solution to seek, real-time, parental authorization when an end-user engages with the IPTV system for CoD selection and if the User profile of that end-user indicates such a need.

Section 6.8.1 provides an example for a call flow to illustrate the roles played by different entities involved in parental control within the context of a CoD service.

Note that scope of parental control extends beyond CoD service and a similar approach can be envisaged for other services, leading eventually to a parental control framework.

6.8.1 Browser-Based Portal CoD Application

This use case is about an end user engaging with the IPTV system for the purpose of selecting a CoD and for whom parental control has been activated in the IPTV service profile.

The call flow for this use case is shown in Figure 6-28. The following is a brief description of the steps:

1. The end user, through the GUI and the OITF, browses the CoD application and makes his choice regarding a CoD.

   The CoD application verifies with the IPTV Service Profile if parental authorization is required, and determines that it is needed in this case.

2. The CoD application returns an HTTP response to the OITF to inform the user that parental authorization is currently being sought, before the selected content can be made available for viewing.

3. The CoD application sends a request to the IPTV Control FE to request parental authorization for the subject end-user. The CoD application includes all information needed in that regard.

   The IPTV Control FE can use various means to obtain the required authorization. For example, IMS communication services, such as SIP messaging, or SMS can be used to obtain such an authorization. Other means can also be envisaged such as e-mail.

4. Once the CoD application receives such an authorization, it can send a SIP MESSAGE to the end-user to indicate that parental authorization is granted.

   Following that, a normal Unicast VoD session is established for the desired content.

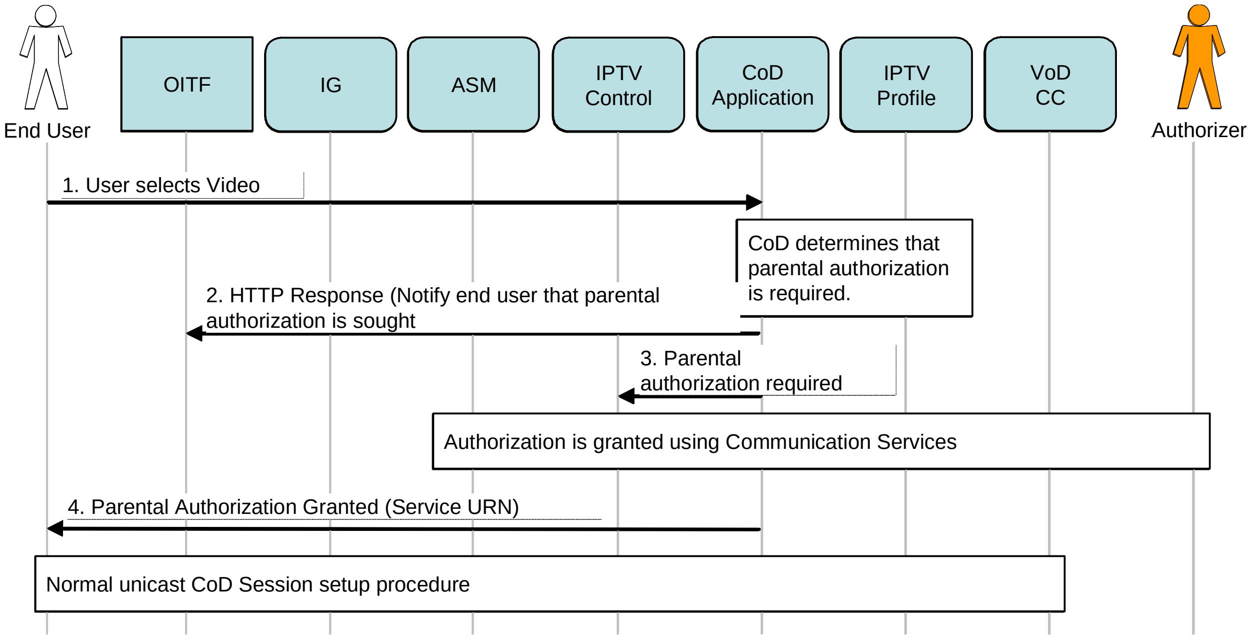

End User
OITF
IG
ASM
IPTV Control
CoD Application
IPTV Profile
VoD CC
Authorizer
1. User selects Video
CoD determines that parental authorization is required.
2. HTTP Response (Notify end user that parental authorization is sought
3. Parental authorization required
Authorization is granted using Communication Services
4. Parental Authorization Granted (Service URN)
Normal unicast CoD Session setup procedure

Figure 6-28: Parental Control for Browser Based CoD Portal

6.9 Service and Content Protection

For service and content protection, this specification supports two approaches:

1. a *terminal-centric* approach that is Marlin-based, that uses OMA file formats (PDCF, DCF) and the Marlin IPMP file format for protection of files, and that supports AES or DVB-CSA encryption, the ECM from IEC 62455 [Ref 32] for MPEG-2 transport stream protection; and

2. a *gateway-centric* approach that is based on a secure authenticated channel between the CSPG and the OITF. The CSP Gateway (CSPG) functional entity supports a framework enabling alternatives to the Marlin based content and service protection solution.

6.9.1 Terminal-centric Content and Service Protection

In the terminal-centric approach, the CSP function in the OITF and the CSP-T Server functional entity on the Provider Network exchange messages related to service and content protection over the UNIS-CSP-T reference point.

6.9.2 Gateway-centric Content and Service Protection

In the gateway-centric approach, the CSP Gateway (CSPG) functional entity inside the Residential Network and the CSP-G Server functional entity on the Provider Network exchange messages related to service and content protection over the UNIS-CSP-G reference point. The HNI-CSP reference point between CSPG and OITF(s) allows the OITF to access CSPG functions for the conversion from a content and service protection scheme to a secure authentication channel between the CSPG and the OITF. The HNI-AGC reference point provides the connection between the CSPG and the Application Gateway (AG).

7. Interworking between IPTV and Communication Services (Informative)

7.1 Caller ID

The Communication Service Caller ID feature allows the display on an OITF of the Caller Id for an incoming voice call. When a user receives a voice call, information related to the Caller ID is sent to the Caller ID enabler from the network managing the call. Using session management procedures, the OITF is able to display the caller's identity (and the called identity, if needed) on the OITF display device.

In a managed network, it is important to ensure that:

- The user has subscribed to such a service, for all identities and E.164 numbers [Ref 20] (POTS, IMS phone, SIP phones, etc) for which he would like to receive Caller ID notifications.
- The networks (POTS, mobile, IMS) managing the identities and the incoming calls, are able to notify the IPTV Control server of information related to incoming voice calls.
- The Caller ID enabler FE, upon receiving this notification, can generate and send a message to the OITF, in order to display the related call information.

The notification mechanism between the Voice Network and the Caller ID enabler is out of scope of this specification.

Figure 7-1 shows an informational call flow for the Caller ID communication service.

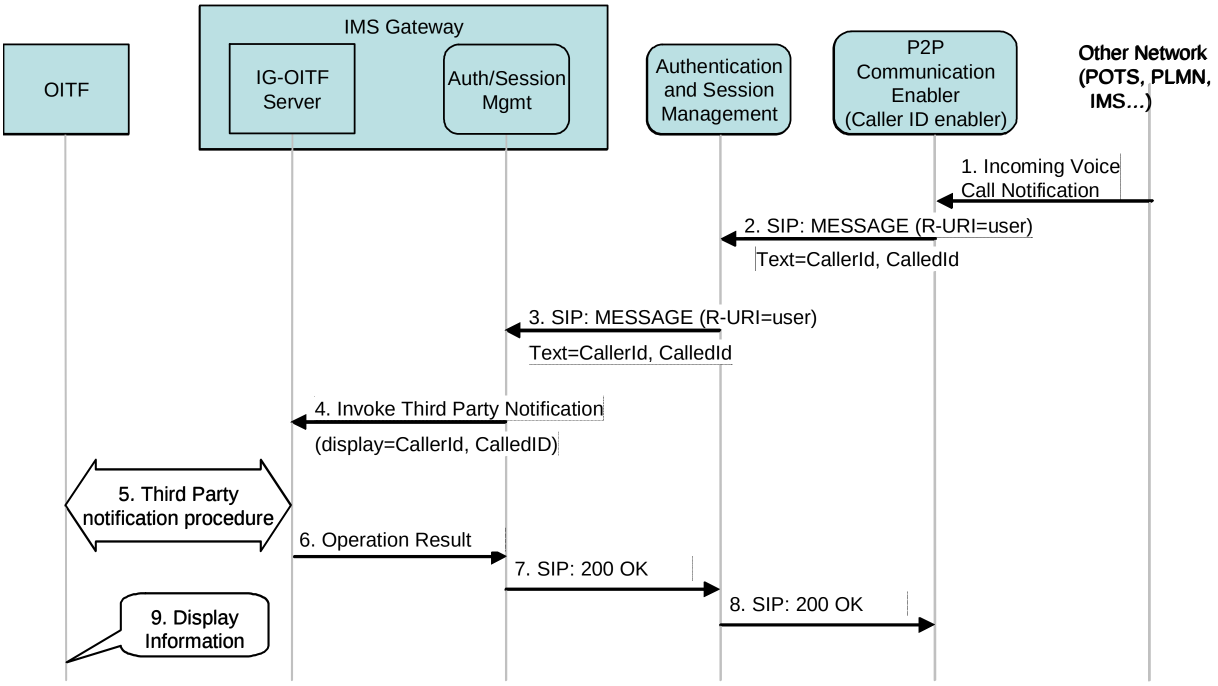

IMS Gateway
OITF
IG-OITF Server
Auth/Session Mgmt
Authentication and Session Management
P2P Communication Enabler (Caller ID enabler)
Other Network (POTS, PLMN, IMS...)
1. Incoming Voice Call Notification
2. SIP: MESSAGE (R-URI=user)
Text=CallerId, CalledId
3. SIP: MESSAGE (R-URI=user)
Text=CallerId, CalledId
4. Invoke Third Party Notification
(display=CallerId, CalledID)
5. Third Party notification procedure
6. Operation Result
7. SIP: 200 OK
8. SIP: 200 OK
9. Display Information

Figure 7-1: Call flow for presentation of caller ID

The following is a brief description of the steps in the flow. As a precondition, the User must be IMS registered via the Authentication and Session Management prior to the call flow.

1. A network (POTS, PLMN, IMS …) notifies the Caller ID enabler about an incoming voice call related to a POTS, PLMN, IMS number/identity associated with an IPTV *user*. This message contains the caller's identity (*caller ID*) and called identity (*called ID*), but should also carry additional information (i.e. the network originating the notification, etc.)

2. The Caller ID enabler generates and sends a SIP MESSAGE (that includes the *caller Id*, the *called Id*, additional information) towards the Authentication and Session Management FE associated with the End User.

3. The SIP MESSAGE is proxied to the IMS Gateway, where it is intercepted by the Authentication and Session management function.

4. The Auth/Session Mgmt. function in the IG invokes the third party notification functionality of the IG-OITF Server function.

5. The IG-OITF Server function starts the notification procedure via the DAE.

   Two possible mechanisms for notifying the OITF are:

   - "Third Party Notification Procedure": With this mechanism the IG-OITF-Server sends the appropriate CEA-2014 [Ref 3] operations so that the OITF can display the appropriate message. In more detail:

     - The IG-OITF Server creates locally the notification message (UPnP multicast) and sends it to the OITF. This message contains the reference/link to the "notification content".

     - The OITF receives the notification message and loads, from the IG-OITF Server, the content referred by the "notification content". In this case, the "notification content" contains the information to be loaded and displayed on the OITF.

     - The OITF sends the response to the IG-OITF-Server after the "notification content" has loaded;

   - Use of UPnP GENA [Ref 28]

6. The IG-OITF Server reports the Operation Result to the Authentication and Session Management. function in the IMS Gateway.

7-8. The response to the MESSAGE request is forwarded to the Caller ID enabler via the Authentication and Session Management FE.

9. The OITF displays the information on the screen.

7.2 Messaging

The Communication Service Messaging allows a user to send and receive textual messages to and from other users (or a list of users). When a user receives a textual message, it is displayed by the OITF on the screen.

The messages are sent and received without initiating a communication context; thus no communication context state is stored in the IPTV Solution.

In order to support the Communication Service Messaging, an Instant Messaging Enabler functionality is used in the Person-to-Person Communication Enablers FE.

The Open Mobile Alliance (OMA) has specified an enabler for Instant Messaging (IM) that allows the exchange of Instant Messaging messages between users in near real-time, based on the IETF SIP protocol [RFC3261] [Ref 21] with SIMPLE and 3GPP extensions. The procedure described in this chapter is aligned with the "Pager mode" functionality as specified in OMA "Instant Messaging using SIMPLE" (OMA-ERP-SIMPLE_IM-V1_0-20070816-C) [Ref 22].

The application running on the OITF sends and receives messages using either:

- A DAE application (HTML + ECMAscript [Ref 23]) downloaded to the OITF

or

- A native application on the OITF

7.2.1 Outgoing messaging

Figure 7-2 shows an example of outgoing messaging communication service, followed by a brief description of the flow.

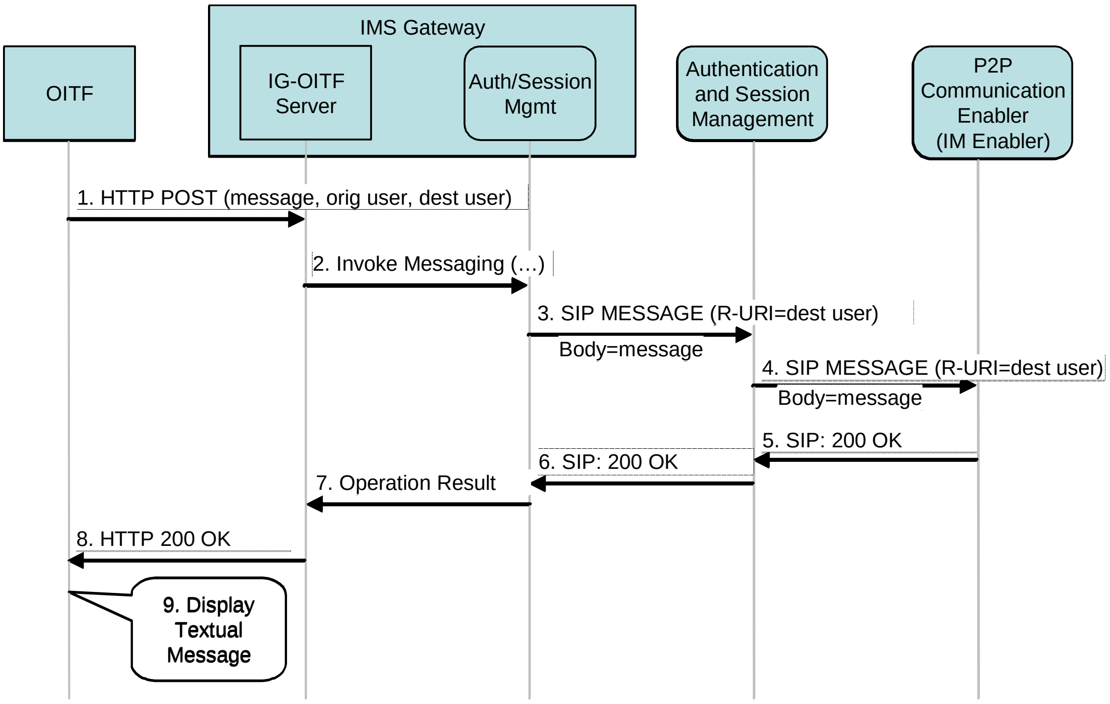

IMS Gateway
OITF
IG-OITF Server
Auth/Session Mgmt
Authentication and Session Management
P2P Communication Enabler (IM Enabler)
1. HTTP POST (message, orig user, dest user)
2. Invoke Messaging (…)
3. SIP MESSAGE (R-URI=dest user)
Body=message
4. SIP MESSAGE (R-URI=dest user)
Body=message
5. SIP: 200 OK
6. SIP: 200 OK
7. Operation Result
8. HTTP 200 OK
9. Display Textual Message

Figure 7-2: Call flow for an outgoing messaging communications service

1. A user logged onto an OITF enters the text message. The OITF sends an HTTP POST message including the text to be sent, the originating user identification and the receiving user identification (or list of users) to the IG-OITF Server function in the IG.

2. The IG-OITF Server function intercepts the HTTP request and invokes the Authentication/Session Management function in the IG to send the text.

3. The Authentication/Session Management function in the IG composes a SIP MESSAGE (that includes the textual message) and sends it to the user’s home Authentication and Session Management FE.

4. Based on the originating filter criteria with the user, the SIP MESSAGE is forwarded to the appropriate IM Enabler FE. This IM Enabler FE is in charge of the delivery the text message to the final receiver or receivers in the list.

5. A 200 OK is received as a response from the terminating network.

6. The 200 OK is proxied to the IMS Gateway.

7. The IG Auth/Session Mgmt function sends the operation result to the IG-OITF Server.

8. The IG-OITF Server sends a 200 OK to the OITF as a response to the HTTP POST operation.

9. The OITF displays the information result on the screen.

7.2.2 Incoming messaging

Figure 7-3 shows an example of incoming messaging communication service, followed by a brief description of the flow.

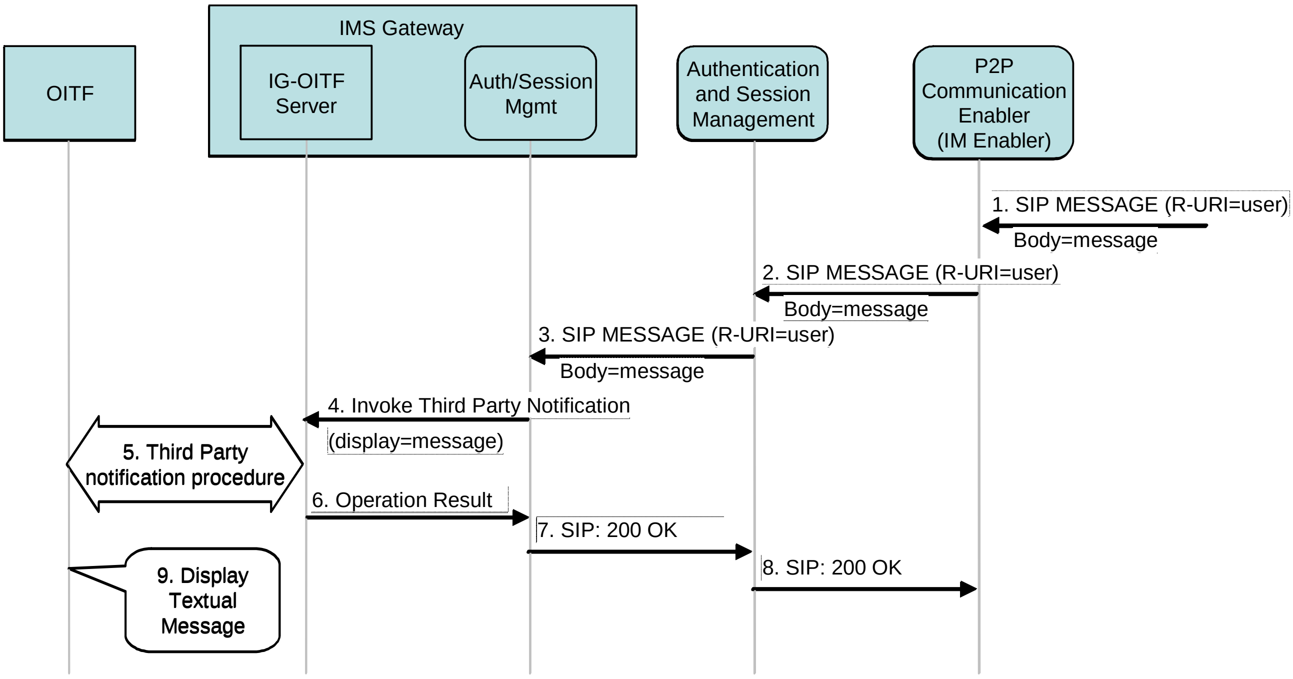

IMS Gateway
OITF
IG-OITF Server
Auth/Session Mgmt
Authentication and Session Management
P2P Communication Enabler (IM Enabler)
1. SIP MESSAGE (R-URI=user)
Body=message
2. SIP MESSAGE (R-URI=user)
Body=message
3. SIP MESSAGE (R-URI=user)
Body=message
4. Invoke Third Party Notification
(display=message)
5. Third Party notification procedure
6. Operation Result
7. SIP: 200 OK
8. SIP: 200 OK
9. Display Textual Message

Figure 7-3: Call flow for an incoming messaging communications service

1. A text message has been sent to the user and arrives to the IM Enabler function, responsible for managing the message delivery to the final receiver (or the users belonging to list).

2. The IM Enabler function sends a SIP MESSAGE (that includes the text message that will be displayed via the OITF) to Authentication and Session Management.

3. The SIP MESSAGE is proxyed to the user IMS Gateway, where it is intercepted by the Auth/Session Mgmt function in the IG.

4. The IG Auth/Session Mgmt function invokes the third party notification functionality in the IG-OITF Server function.

5. The IG-OITF Server starts the Third Party Notification Procedure. In particular the IG-OITF sends the appropriate CEA-2014 [Ref 3] operations so that the OITF displays the appropriate message. In more detail:

   a. The IG-OITF Server function creates locally the notification message (multicast) and sends it to the OITF. This message contains the reference/link to the “notification content”.

   b. The OITF receives the notification message and loads, from the IG-OITF Server, the content referred to by the “notification content”. In this case, the “notification content” contains the information to be loaded and displayed on the OITF.

   c. OITF sends the response to the IG-OITF Server function in the IG after the “notification content” loading;

6. The IG-OITF Server reports the Operation Result to the IG Auth/Session Mgmt function in the IMS Gateway.

7-8. The response to the MESSAGE request is forwarded to the other network via Authentication and Session Management.

9. The OITF displays the information on the screen.

7.3 Chatting

The Communication Service Chatting allows a user to establish a communication context with another user or with a group of users, so that the IPTV Solution allows the user to send textual messages within a communication context and have all other users in that context receive the message.

The messages are sent/received within a communication context; the state of the communication context is stored in the IPTV Solution.

In order to support the Communication Service Chatting, an Instant Messaging Enabler functionality is introduced. OMA (Open Mobile Alliance) has specified an enabler for Instant Messaging (IM) that allows the exchange of Instant Messaging messages between users in near real-time, based on the IETF SIP protocol [RFC3261] [Ref 21] with SIMPLE and 3GPP extensions. The procedure described in this chapter is aligned with the "Session mode" functionality as specified in OMA "Instant Messaging using SIMPLE" (OMA-TS-SIMPLE_IM-V1_0-20070816-C) [Ref 22].

7.3.1 Chat session setup

Figure 7-4 shows an example of a chatting session set-up (i.e. communication context set-up), followed by a brief description of the flow. In this case the chatting template is generated and presented to the user directly by the OITF. The chatting template could be also generated by the IG, with a procedure including initial steps analogous to the ones presented in Section 7.4.2.1.

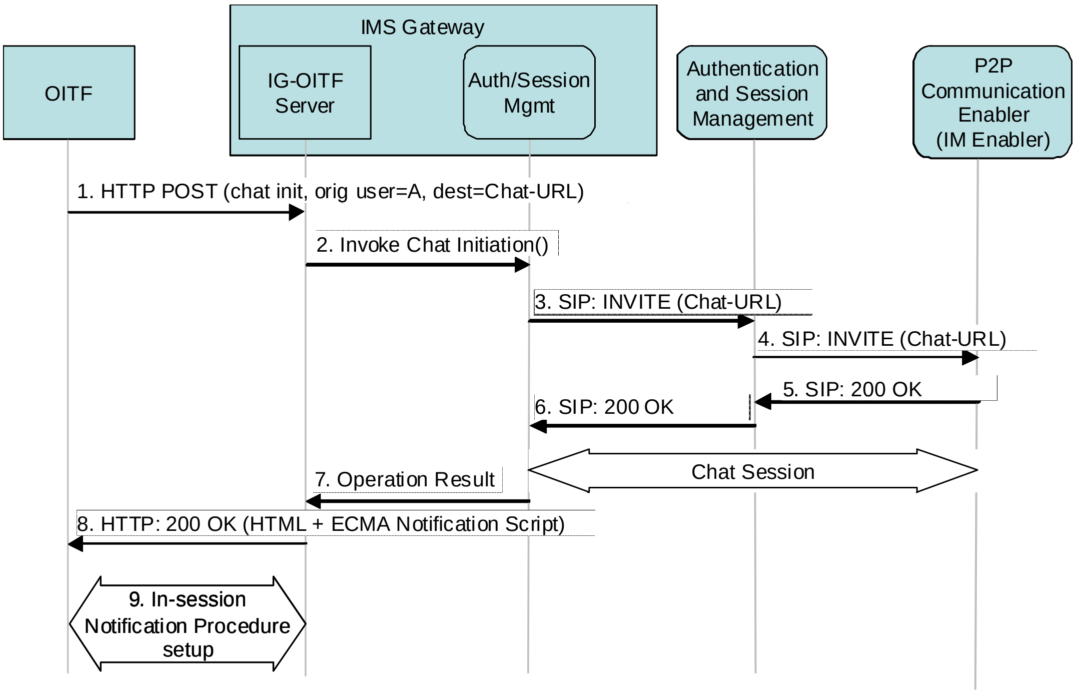

IMS Gateway
OITF
IG-OITF Server
Auth/Session Mgmt
Authentication and Session Management
P2P Communication Enabler (IM Enabler)
1. HTTP POST (chat init, orig user=A, dest=Chat-URL)
2. Invoke Chat Initiation()
3. SIP: INVITE (Chat-URL)
4. SIP: INVITE (Chat-URL)
5. SIP: 200 OK
6. SIP: 200 OK
Chat Session
7. Operation Result
8. HTTP: 200 OK (HTML + ECMA Notification Script)
9. In-session Notification Procedure setup

Figure 7-4: Call flow for Chat session setup

1. A user logged onto an OITF wants to set up a chat session. The OITF presents a template to be filled up by the user; the user fills the template and the OITF sends an HTTP POST message including the needed information (e.g. originating user and the Chat-URL) to the IG-OITF server.

2. The IG-OITF Server intercepts the HTTP request and invokes the IG Auth/Session Mgmt function to set up a chat session.

3, 4. The IG Auth/Session Mgmt function composes a SIP INVITE (including the originating user and the Chat-URL) and sends it to the user's home Authentication and Session Management FE in order to establish a chat session.

The SIP INVITE is proxied to the IM Enabler function that manages the chat session (The details of SIP message exchange are not shown here).

5,6. A 200 OK is received as a response from the IM Enabler function and it is proxied to IMS Gateway, and a chat session is established between the IG and the IM Enabler.

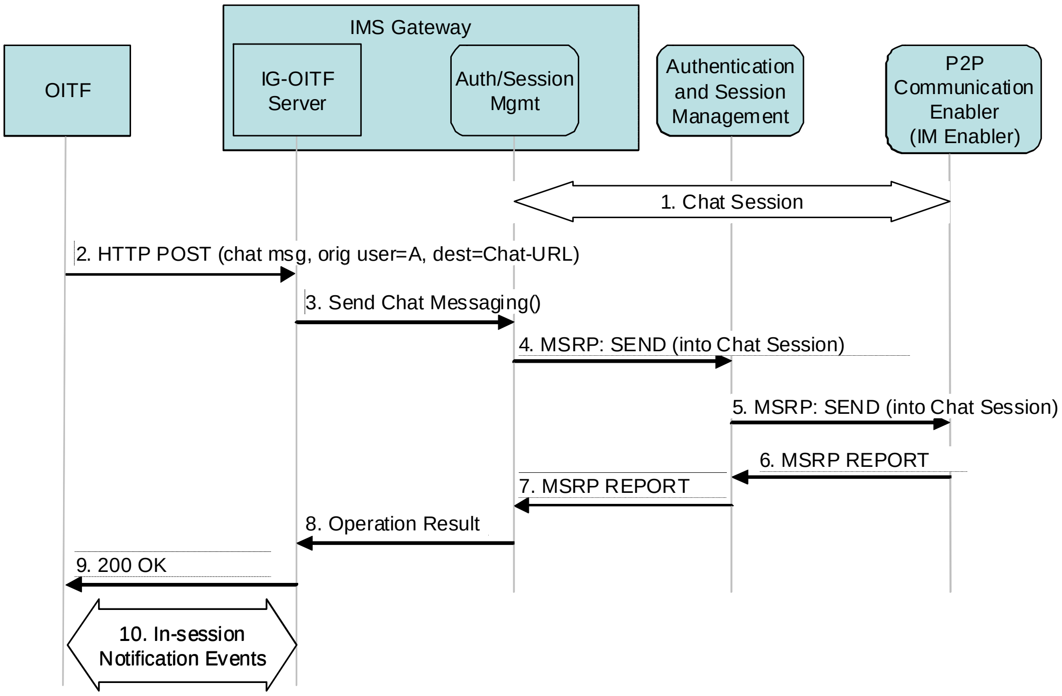
7. The IG Auth/Session Mgmt function sends the operation result to the IG-OITF Server function.

8. The IG-OITF Server subsequently sends a 200 OK to the OITF as a response to the HTTP POST operation, containing the result page (which will be updated when a chat event is received) and an ECMA Notification Script, that will be run by the client in order to set-up an In-Session Notification Procedure.

9. The OITF sets up an In-Session Notification Procedure (XML HTTP request or Persistent TCP Connection Mode) with the IG-OITF Server function in the IG. The IG-OITF Server function will then be able to send a notification message to update the OITF UI page dynamically without the need to reload the XHTML page.

7.3.2 Chat outgoing message

Figure 7-5 shows an example of chat outgoing message, followed by a brief description of the flow.



IMS Gateway
OITF
IG-OITF Server
Auth/Session Mgmt
Authentication and Session Management
P2P Communication Enabler (IM Enabler)
1. Chat Session
2. HTTP POST (chat msg, orig user=A, dest=Chat-URL)
3. Send Chat Messaging()
4. MSRP: SEND (into Chat Session)
5. MSRP: SEND (into Chat Session)
6. MSRP REPORT
7. MSRP REPORT
8. Operation Result
9. 200 OK
10. In-session Notification Events

Figure 7-5: Call flow for a Chat outgoing message

1. A user logged on an OITF has already established a chat session (for details, see section 7.3.1) with the IM Enabler function for a specific Chat-URL.

2. A user wants to send a text message in that chat session. The OITF sends an HTTP POST message including the information needed (text to be sent, the originating user and Chat-URL, etc.) to the IG-OITF Server.

3. The IG-OITF Server intercepts the HTTP request and invokes IG Auth/Session Mgmt function to send the text in a chat session.

4, 5. The IG Auth/Session Mgmt function composes a MSRP SEND message (that includes the text message) and sends it, in the chat session, to the user's home network Authentication and Session Management functional entity. The MSRP SEND message is proxied to the IM Enabler function.

6,7. A MSRP REPORT message is received from the IM Enabler function as a response to the MSRP SEND message, and it is proxied to IMS Gateway.

8. The IG Auth/Session Mgmt sends the operation result to the IG-OITF server.

9. The IG-OITF Server subsequently sends a 200 OK to the OITF as a response to the HTTP POST operation.

10. The IG-OITF Server, if needed, performs the necessary CEA-2014 [Ref 3] operation so that the OITF displays the result information on the screen, using the In-Session Notification established earlier during the chat session set-up procedure.

7.3.3 Chat incoming message

Figure 7-6 shows an example of a chat incoming message, followed by a brief description of the flow.

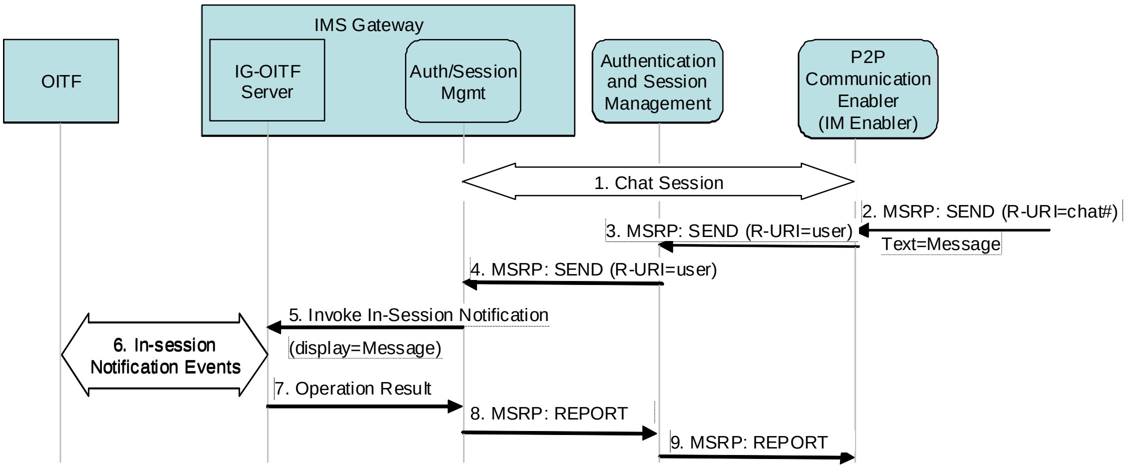

IMS Gateway
OITF
IG-OITF Server
Auth/Session Mgmt
Authentication and Session Management
P2P Communication Enabler (IM Enabler)
1. Chat Session
2. MSRP: SEND (R-URI=chat#)
Text=Message
3. MSRP: SEND (R-URI=user)
4. MSRP: SEND (R-URI=user)
5. Invoke In-Session Notification
(display=Message)
6. In-session Notification Events
7. Operation Result
8. MSRP: REPORT
9. MSRP: REPORT

Figure 7-6: Call flow for a Chat incoming session

1. A user logged on an OITF has already established a chat session (for details see section 7.3.1) with the IPTV Control.

2. The IM Enabler function receives a MSRP SEND message (that includes the message to be delivered to the OITF) from another user in the chat session (identified by a Chat-URL).

3, 4. The MSRP SEND message is proxied via Authentication and Session Management to the user’s IMS Gateway, where it is intercepted by the IG Auth/Session Mgmt function.

5. The IG Auth/Session Mgmt function invokes the In-session Notification functionality in the IG-OITF Server.

6. The IG-OITF Server performs the necessary CEA-2014 [Ref 3] operation so that the OITF displays the message on the screen, using the In-Session Notification established earlier during the chat session set-up procedure.

7. The IG-OITF Server reports the Operation Result to the IG Auth/Session Mgmt function on the IMS Gateway.

8,9. Finally, the MSRP REPORT, in response to the MSRP SEND message, is forwarded to IM Enabler via the Authentication and Session Management FE.

7.3.4 Chatting session teardown

When the user wants to end the chat session, he performs the needed actions on the OITF (e.g. pushing a button). This causes:

- the In-session Notification tear down;
- a terminating message to be sent to the IG;

- the tear down of the chat session between the IG and the IM Enabler, through standard IM session-mode and IMS tear-down procedures.

7.4 Presence

7.4.1 General Description of Presence in IPTV

IPTV services may be combined with Presence service capability. The mechanisms used in order to combine IPTV services with the Presence service capabilities may also be used for other purposes such as:

- Gathering channel statistics and user behaviour information.
- Supporting session continuity between different terminals

The ITF must be able to collect and send Presence information related to:

- the end user (e.g. status of the end user);
- the IPTV service activated (e.g. Scheduled Content, CoD, PVR);
- the IPTV program watched (e.g. channel currently accessed, program currently watched, content currently accessed);
- other information the ITF can manage (e.g. in case of a hybrid ITF - IPTV and DTT capable - channel/program accessed/watched on DTT; in case of a combined deployment – unmanaged and managed models are both enabled – channel/program accessed via an unmanaged network).

It is the user's decision (through the use of privacy preferences) as to which specific IPTV attributes to include in the Presence information that is made available to other users.

Figure 7-7 and Figure 7-9 show two examples of the use of the Presence service with IPTV.

Figure 7-7 shows the mechanism proposed in order to allow an ITF to communicate Presence information.

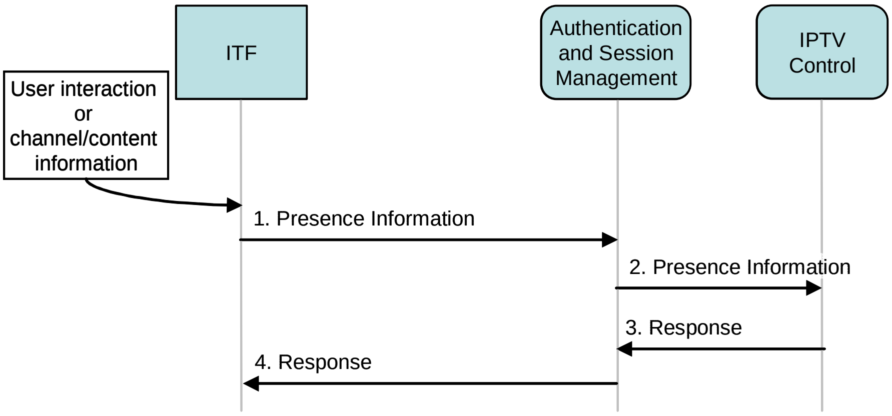

ITF
Authentication and Session Management
IPTV Control
User interaction or channel/content information
1. Presence Information
2. Presence Information
3. Response
4. Response

Figure 7-7: Call flow for sending Presence information to IPTV Control

The IPTV Control can forward and aggregate the Presence information collected towards other entities (e.g. external Presence Server, other specific application server) based on internal policies/rules.

The ITF may also collect and send the IPTV Presence information to the P2P Communication Enabler (Presence Enabler) directly, as shown in Figure 7-8.

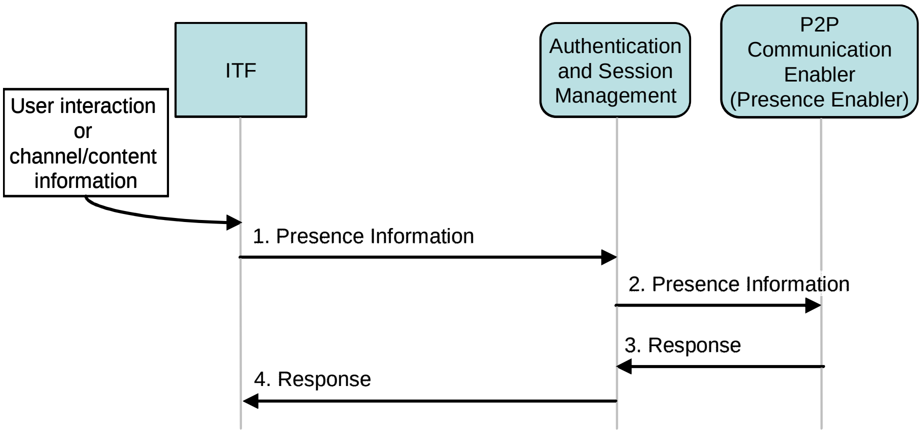

ITF
Authentication and Session Management
P2P Communication Enabler (Presence Enabler)
User interaction or channel/content information
1. Presence Information
2. Presence Information
3. Response
4. Response

Figure 7-8: Call flow for sending Presence information to the Presence Enabler

7.4.2 Presence Session Management Procedures

The Communication Service Presence allows multiple users of an ITF to communicate their presence information inside an IPTV Service network. A user (A) can subscribe to the presence information of other users (B,C …) so that when one of these users changes his Presence status user (A) will receive a notification of this change.

The OMA (Open Mobile Alliance) has specified an enabler for Presence allowing the management of the collection and the controlled dissemination of presence information over a SIP/IP network. The enabler is based on the IETF SIP protocol [RFC3261] [Ref 21] with SIMPLE and 3GPP extensions. The procedure described in this section is aligned with the procedures specified in OMA “Presence SIMPLE Specification” (OMA-ERP-Presence_SIMPLE-V1_0_1-20061128-A) [Ref 24]

7.4.2.1 Presence session set-up – Presence template produced by the IG

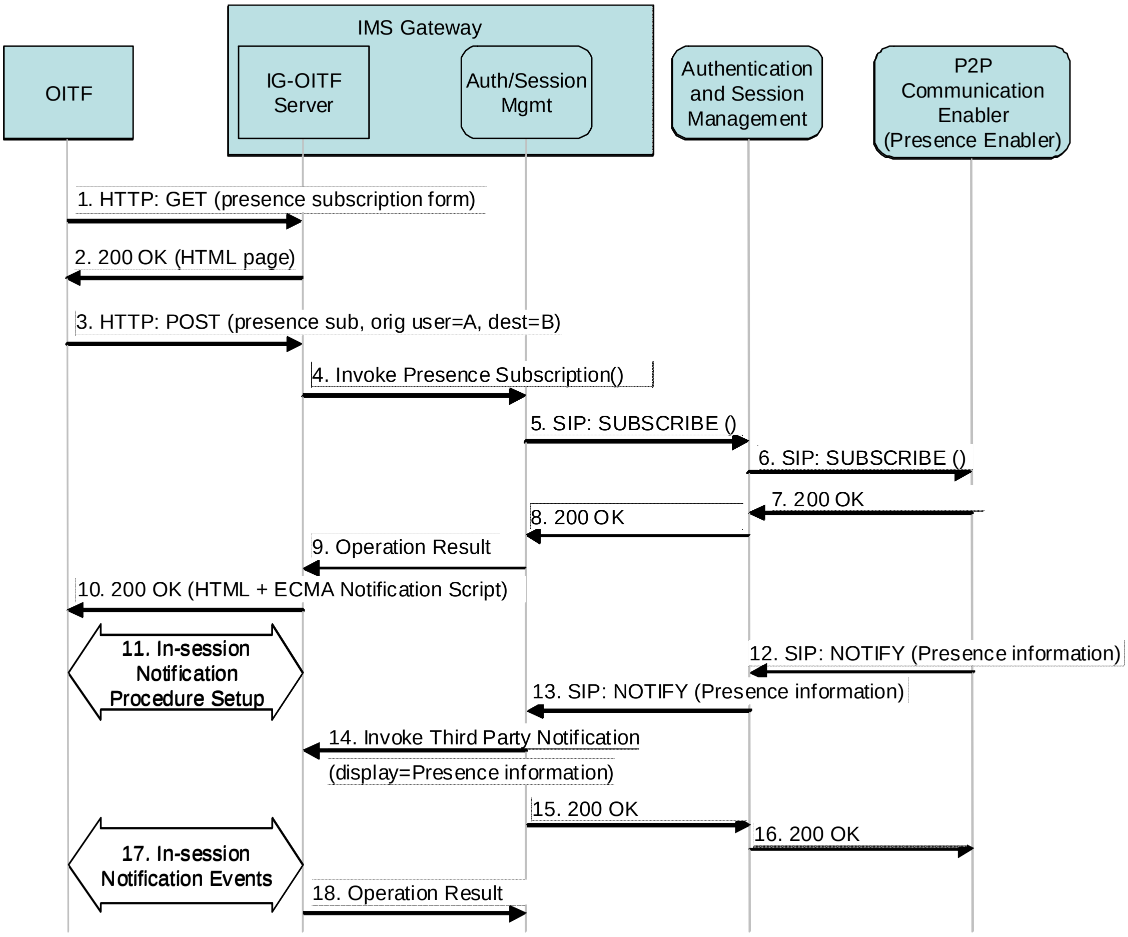

IMS Gateway
OITF
IG-OITF Server
Auth/Session Mgmt
Authentication and Session Management
P2P Communication Enabler (Presence Enabler)
1. HTTP: GET (presence subscription form)
2. 200 OK (HTML page)
3. HTTP: POST (presence sub, orig user=A, dest=B)
4. Invoke Presence Subscription()
5. SIP: SUBSCRIBE ()
6. SIP: SUBSCRIBE ()
7. 200 OK
8. 200 OK
9. Operation Result
10. 200 OK (HTML + ECMA Notification Script)
11. In-session Notification Procedure Setup
12. SIP: NOTIFY (Presence information)
13. SIP: NOTIFY (Presence information)
14. Invoke Third Party Notification
(display=Presence information)
15. 200 OK
16. 200 OK
17. In-session Notification Events
18. Operation Result

Figure 7-9: Call flow for Presence session setup

The following is a brief description of the steps in the flow:

1. A user logged on to an OITF wants to subscribe to the presence events associated with another user or a group of users. The OITF sends an HTTP GET message that allows it to fetch a template form to be filled up by the user.

2. The IG-OITF Server intercepts the request and returns an HTML form document to be filled out by the end user in a 200 OK message.

3. The OITF sends an HTTP POST message including the completed template form to the IG-OITF Server.

4. The IG-OITF Server intercepts the message and invokes the appropriate operation in the Auth/Session Mgmt. function in the IG.

5. The Auth/Session Mgmt. function in the IG creates a SIP SUBSCRIBE message with the appropriate information and sends it to the Authentication and Session Management FE in the user’s home network.

6. A SIP SUBSCRIBE message is forwarded to the Presence Enabler function.

7. A 200 OK is received as a response from the Presence Enabler function.

8. A 200 OK is forwarded to the Auth/Session Mgmt. function in the IG.

9. The Auth/Session Mgmt. function in the IG sends the operation result to the IG-OITF Server.

10. The IG-OITF Server sends a 200 OK to the OITF as a response to the HTTP POST operation, which contains the result page (which will be updated when a presence event is received) and an ECMA Notification Script that is run by the client in order to set-up an In-Session Notification Procedure.

11. The OITF sets up an In-Session Notification Procedure (XML HTTP request or Persistent TCP Connection Mode) with the IG-OITF Server. The IG-OITF Server will then be able to send a notification message to update the OITF UI page dynamically without the need to reload the XHTML-page.

12, 13.The Auth/Session Mgmt. function in the IG receives a NOTIFY message that includes the Presence status from Presence Enabler function via Authentication and Session Mgmt. function.

14. The Auth/Session Mgmt. function in the IG invokes the In-session notification function in the IG-OITF Server.

15. The Auth/Session Mgmt. function in the IG sends 200 OK message to Authentication and Session Mgmt. function in responds to the SIP NOTIFY.

16. A 200 OK is forwarded to Presence Enabler function..

17. The IG-OITF Server performs the necessary in-session notification operation (CEA-2014) [Ref 3] for the OITF to display the presence information to the end-user. All NOTIFY messages, for this subscription, are delivered within the In-Session Notification session, established in step 9.

18. Finally the IG-OITF Server sends back to the IG Auth/Session Mgmt. function the operation result.

7.4.3 Scheduled Content and fast update rate events case

When channel switching during a Scheduled Content service, users will likely be able to zap between a set of channels within the same “bouquet” (e.g. channel with the same bandwidth requirements) without further signalling related to the Service Setup Session (from ITF to IPTV Control). In this case, sending presence information each time the user changes channel may lead to a heavy load on the network (e.g. in case of zapping). In order to reduce and control possible overload caused by frequent channel hopping, it shall be possible to define some mechanisms that is able to limit the number of publications of channel change. In particular, two instances of mechanisms can be foreseen:

- Client side – configurable delay: the ITF client should not inform the IPTV Control about several consecutive channel changes within the delay period. When the user stops zapping, information about the watched channel should be sent to the IPTV Solution. The delay time that is used may be configurable.

- Server side – rate control: The IPTV Solution should control the rate of information sent by ITF client so it can decrease the frequency of publication of change channel.

Figure 7-10 and Figure 7-11 provide examples of a signalling flow for channel switching, for the case of Client side and Server side load control, respectively.

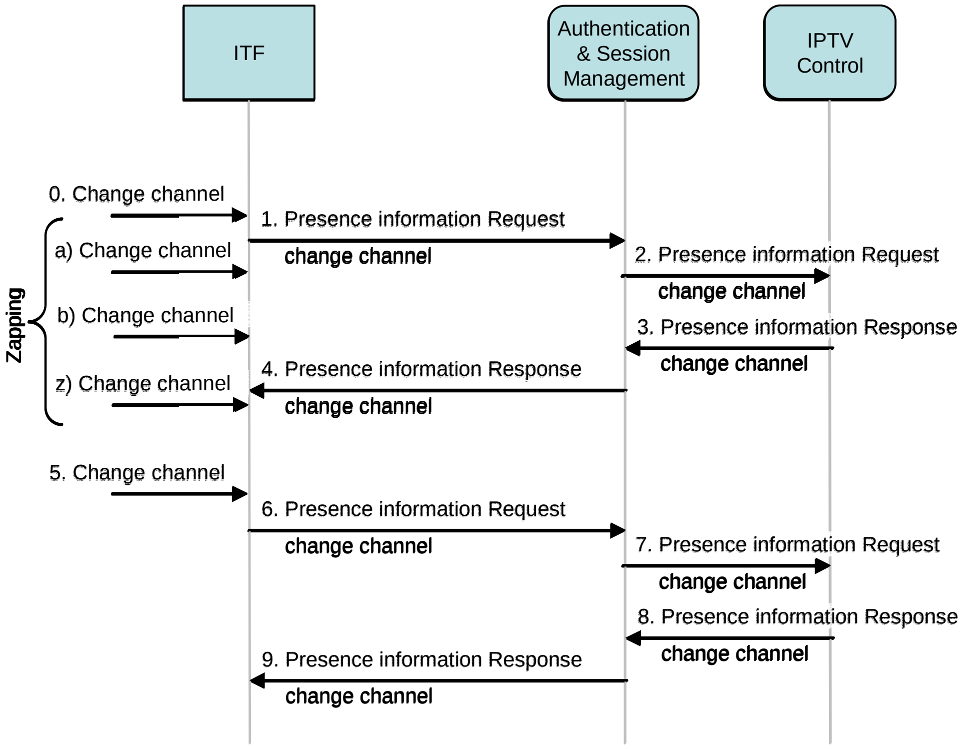

ITF
Authentication & Session Management
IPTV Control
0. Change channel
Zapping
a) Change channel
b) Change channel
z) Change channel
1. Presence information Request
change channel
2. Presence information Request
change channel
3. Presence information Response
change channel
4. Presence information Response
change channel
5. Change channel
6. Presence information Request
change channel
7. Presence information Request
change channel
8. Presence information Response
change channel
9. Presence information Response
change channel

Figure 7-10: Scheduled Content (Broadcast TV) channel switching; Client Side load control

0. The ITF leaves a multicast channel and joins another multicast channel with the same QoS requirements.
   a. A delay may be applied. If the user switches channel again during this delay time, the flow is restarted at step 0.
   b. (see a.)
   c. (see a.)
   d. …
1. The ITF sends information about which channel that is being watched.
2. The Authentication and Session Management FE routes the information to the IPTV Control.
3. IPTV Control responds to the Inform channel change request.
4. The Authentication and Session Management routes the response to the ITF.

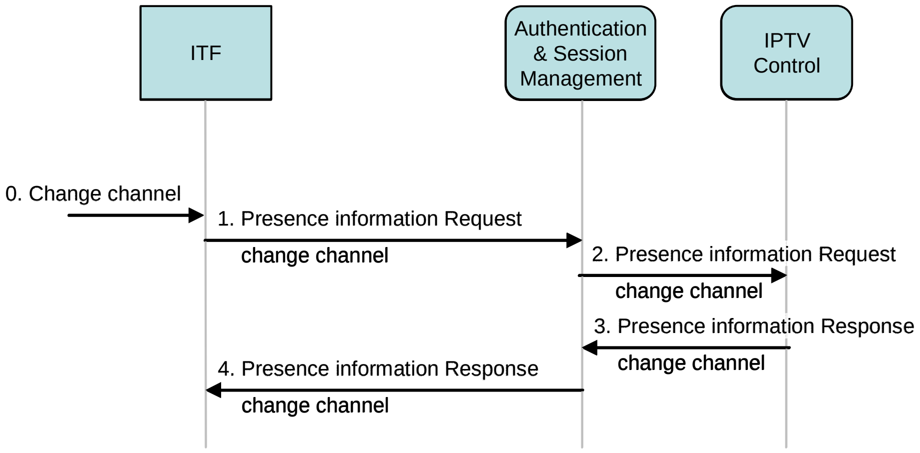

ITF
Authentication & Session Management
IPTV Control
0. Change channel
1. Presence information Request
change channel
2. Presence information Request
change channel
3. Presence information Response
change channel
4. Presence information Response
change channel

Figure 7-11: Scheduled Content (Broadcast TV) channel switching: Server Side load control

0. The ITF leaves a multicast channel and joins another multicast channel.

1. The ITF sends information about which channel is being watched.

2. The Authentication and Session Management FE routes the information to the IPTV Control.

3. IPTV Control checks the rate notification from the ITF and responds to the Inform channel change request; also sent in the response is an info (rate of publication) to decrease the frequency of sending the change channel information.

4. The Authentication and Session Management FE routes the response to the OITF which updates its own rate of publication.

8. Interworking ITF with DLNA devices (Informative)

The following is a high level signal flow which shows how “DLNA functions” in the OITF interwork with DLNA compliant devices. In all use cases described in this section, the DLNA Function in the OITF serves IPTV content to other DLNA devices which implement the appropriate DLNA device class or DLNA device capability. However, in general, “DLNA functions” in the OITF may support other DLNA device classes or DLNA device capabilities, such as DLNA Digital Media Player (DMP), in order to support accessing AV content (which may not be IPTV content) which are served by other DLNA devices. For further information about DLNA system usages, please refer to DLNA Networked Device Interoperability Guidelines (October 2006) [Ref 2].

Basically, the signal flows between the ITF and the Provider(s) Networks are the same as defined by this specification. The signal flow between ITF and DLNA devices are the same as defined in the DLNA guidelines. The high level signal flow in Figure 8-1 is intended to show the relation between the IPTV signal flow and the DLNA signal flow on the assumption that the DLNA function in the OITF converts IPTV protocols, such as metadata access and media delivery protocols, on the fly to DLNA protocols. In the case where the ITF has a local storage, the IPTV content in the storage may be served to DLNA devices; however, the following high level signal flows do not apply to these cases.

The IPTV content item served by the DLNA function can be protected by DTCP-IP, with content usage specified via the content and service protection scheme of the IPTV service.

Note that each call flow between the ITF and the Provider(s) Networks can include an optional authentication step to avoid unauthorized access to IPTV services.

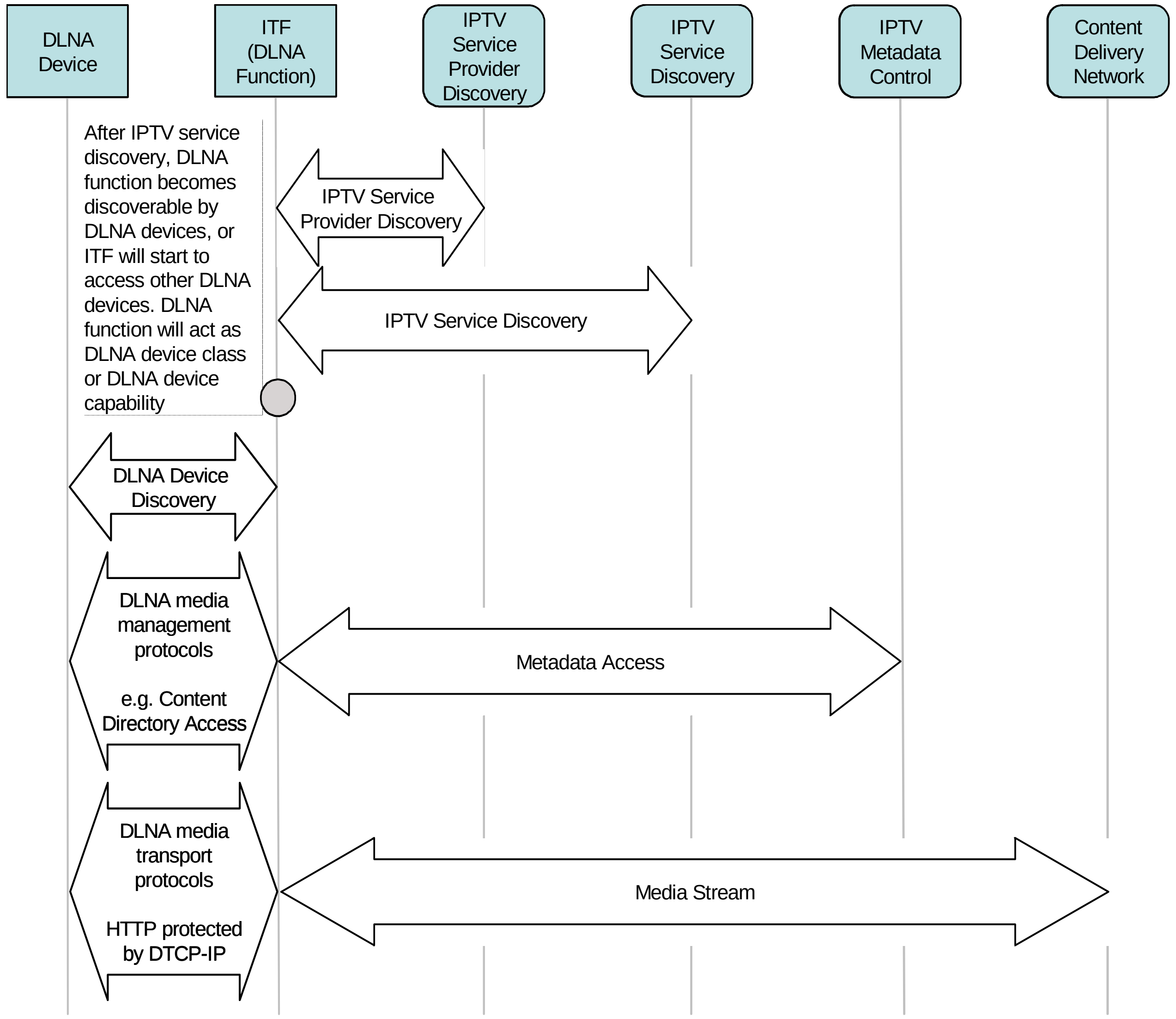

DLNA Device
ITF (DLNA Function)
IPTV Service Provider Discovery
IPTV Service Discovery
IPTV Metadata Control
Content Delivery Network
After IPTV service discovery, DLNA function becomes discoverable by DLNA devices, or ITF will start to access other DLNA devices. DLNA function will act as DLNA device class or DLNA device capability
IPTV Service Provider Discovery
IPTV Service Discovery
DLNA Device Discovery
DLNA media management protocols
e.g. Content Directory Access
Metadata Access
DLNA media transport protocols
HTTP protected by DTCP-IP
Media Stream

Figure 8-1: Relation between the IPTV and the DLNA signal flows

The DLNA guideline defines system usages, i.e. use cases, showing how DLNA device classes and DLNA functions interact with each other. Table 5 indicates what DLNA use cases could be supported and how DLNA device class or DLNA functional capability should be implemented in the DLNA function of the OITF to realize each use case. Note that mobile networked devices, such as M-DMS, M-DMC, are not listed in this table, but a mobile networked device corresponding to a home network device also apply to these system usages as well.

DLNA system usages (use cases)	DLNA function in OITF	DLNA Device(s) which interwork with the DLNA function in the OITF.
2 BOX PULL	Digital Media Server (DMS)	Digital Media Player (DMP)
DOWNLOAD	Digital Media Server (DMS)	Download Controller (+DN+)
3 BOX	Digital Media Server (DMS)	Digital Media Controller (DMC) Digital Media Render (DMR)
	Digital Media Server (DMS) Digital Media Controller (DMC)	Digital Media Renderer (DMR)
2 BOX PUSH	Push Controller (+PU+)	Digital Media Renderer (DMR)
UPLOAD	Upload Controller (+UP+)	Digital Media Server (DMS) with upload capability

Table 5: DLNA system usages

8.1 2 BOX PULL

Figure 8-2 shows the signal flow for the 2 BOX PULL system usage where an OITF serves IPTV content to a DMP. In this system usage, a user operates the DLNA Device which implements the DLNA Digital Media Player (DMP)

The signal flow applies to the case when OITF automatically has access to the IPTV content.

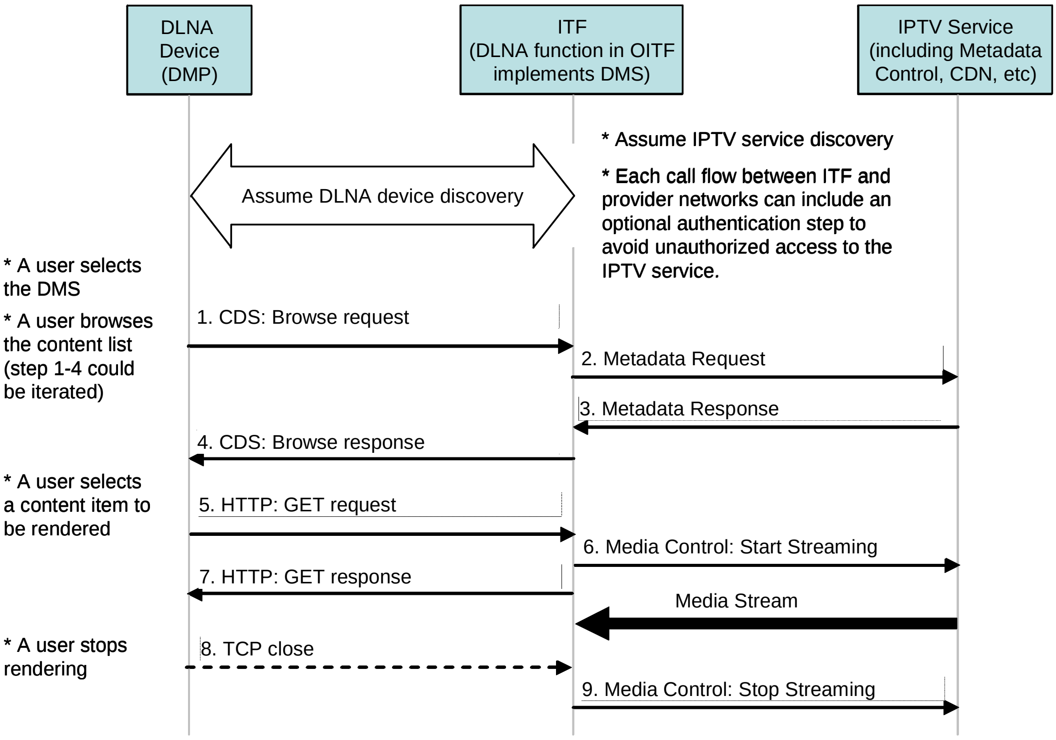

DLNA Device (DMP)
ITF (DLNA function in OITF implements DMS)
IPTV Service (including Metadata Control, CDN, etc)
* Assume IPTV service discovery
* Each call flow between ITF and provider networks can include an optional authentication step to avoid unauthorized access to the IPTV service.
Assume DLNA device discovery
* A user selects the DMS
* A user browses the content list (step 1-4 could be iterated)
1. CDS: Browse request
2. Metadata Request
3. Metadata Response
4. CDS: Browse response
* A user selects a content item to be rendered
5. HTTP: GET request
6. Media Control: Start Streaming
7. HTTP: GET response
Media Stream
* A user stops rendering
8. TCP close
9. Media Control: Stop Streaming

Figure 8-2: Signal flows for a 2 BOX PULL system usage

8.2 DOWNLOAD

The signal flow for DLNA download system usage is the same as for the 2 BOX PULL, except that the DLNA device implements the Download Controller (+DN+) instead of the DMP, and the media delivery on the network side will be based on a file transfer protocol instead of a media streaming protocol. In this system usage, a user operates the DLNA device which implements the DLNA Download Controller (+DN+).

The signal flow shown in Figure 8-3 applies to the case when the OITF automatically has access to the IPTV content.

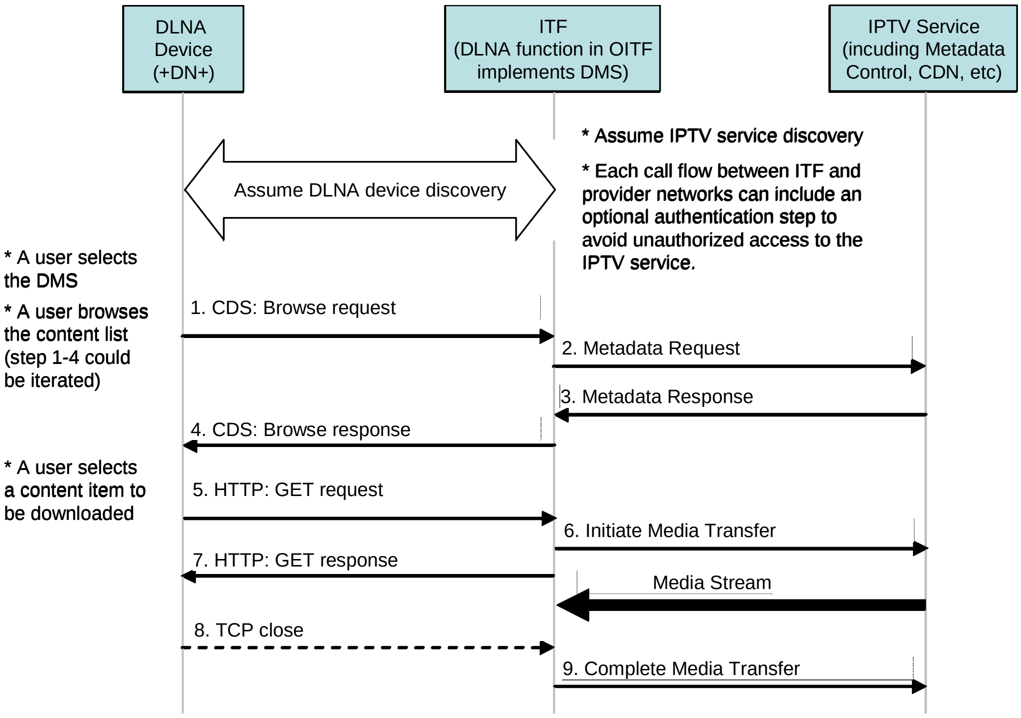

DLNA Device (+DN+)
ITF (DLNA function in OITF implements DMS)
IPTV Service (incuding Metadata Control, CDN, etc)
Assume DLNA device discovery
* Assume IPTV service discovery
* Each call flow between ITF and provider networks can include an optional authentication step to avoid unauthorized access to the IPTV service.
* A user selects the DMS
* A user browses the content list (step 1-4 could be iterated)
1. CDS: Browse request
2. Metadata Request
3. Metadata Response
4. CDS: Browse response
* A user selects a content item to be downloaded
5. HTTP: GET request
6. Initiate Media Transfer
7. HTTP: GET response
Media Stream
8. TCP close
9. Complete Media Transfer

Figure 8-3: Signal flow for DLNA download system

8.3 3 BOX

Figure 8-4 shows the signal flow for the 3 BOX system usage where the ITF acts as a DMS. The two DLNA devices (DMR and DMC) interwork with the DMS implemented in the OITF FE of the ITF. In this system usage, a user operates the DLNA device which implements the DLNA Digital Media Controller (DMC).

The signal flow applies to the case where the OITF automatically has access to the IPTV content.

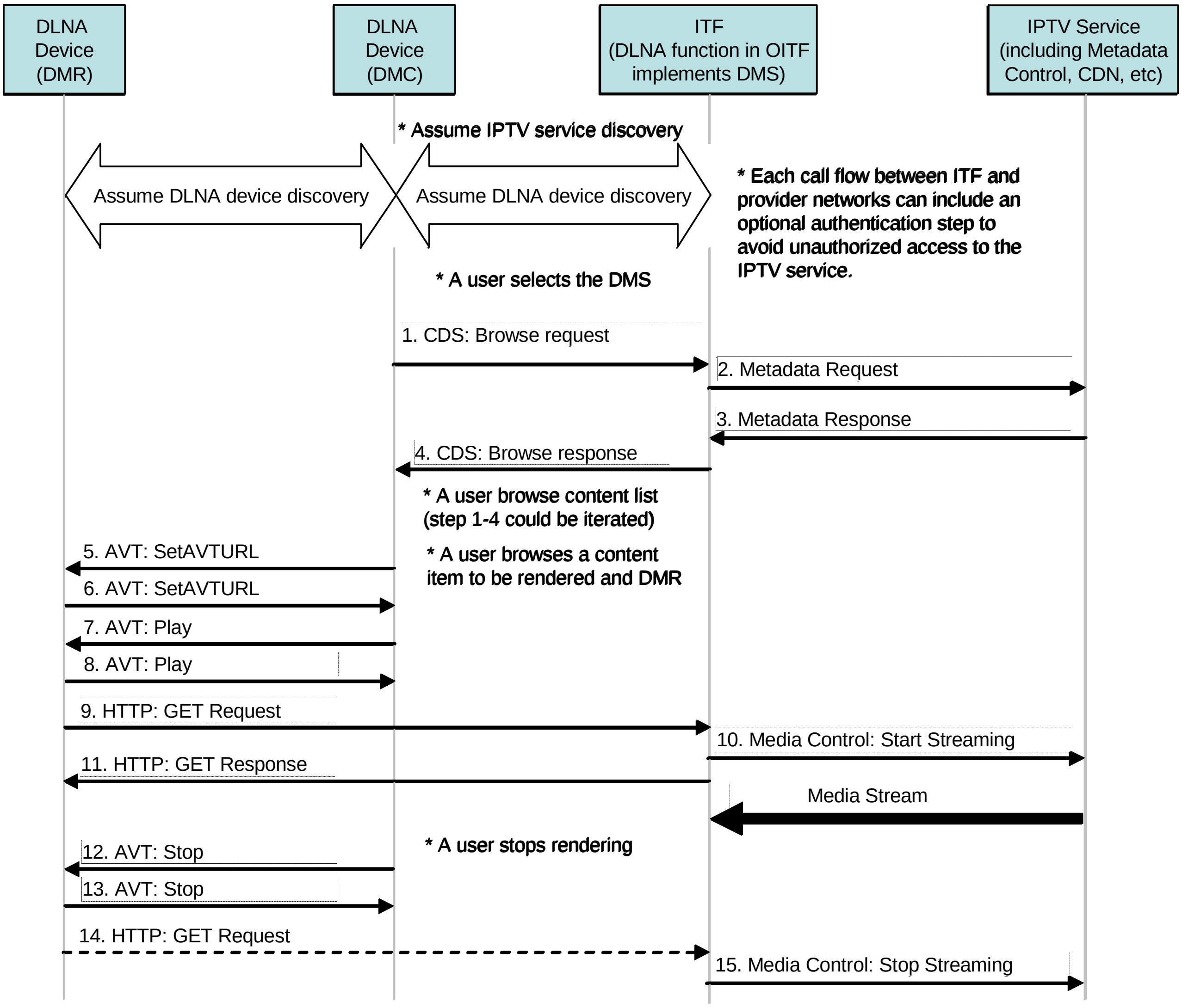

DLNA Device (DMR)
DLNA Device (DMC)
ITF (DLNA function in OITF implements DMS)
IPTV Service (including Metadata Control, CDN, etc)
* Assume IPTV service discovery
Assume DLNA device discovery
Assume DLNA device discovery
* Each call flow between ITF and provider networks can include an optional authentication step to avoid unauthorized access to the IPTV service.
* A user selects the DMS
1. CDS: Browse request
2. Metadata Request
3. Metadata Response
4. CDS: Browse response
* A user browse content list (step 1-4 could be iterated)
5. AVT: SetAVTURL
* A user browses a content item to be rendered and DMR
6. AVT: SetAVTURL
7. AVT: Play
8. AVT: Play
9. HTTP: GET Request
10. Media Control: Start Streaming
11. HTTP: GET Response
Media Stream
12. AVT: Stop
* A user stops rendering
13. AVT: Stop
14. HTTP: GET Request
15. Media Control: Stop Streaming

Figure 8-4: Signal flow for the 3 BOX system usage where the ITF acts as a DMS

Figure 8-5 shows the signal flow for the 3 BOX system usage where the ITF acts as both a DMC and a DMS. In this system usage, a user operates the OITF which implements the DLNA Digital Media Controller (DMC).

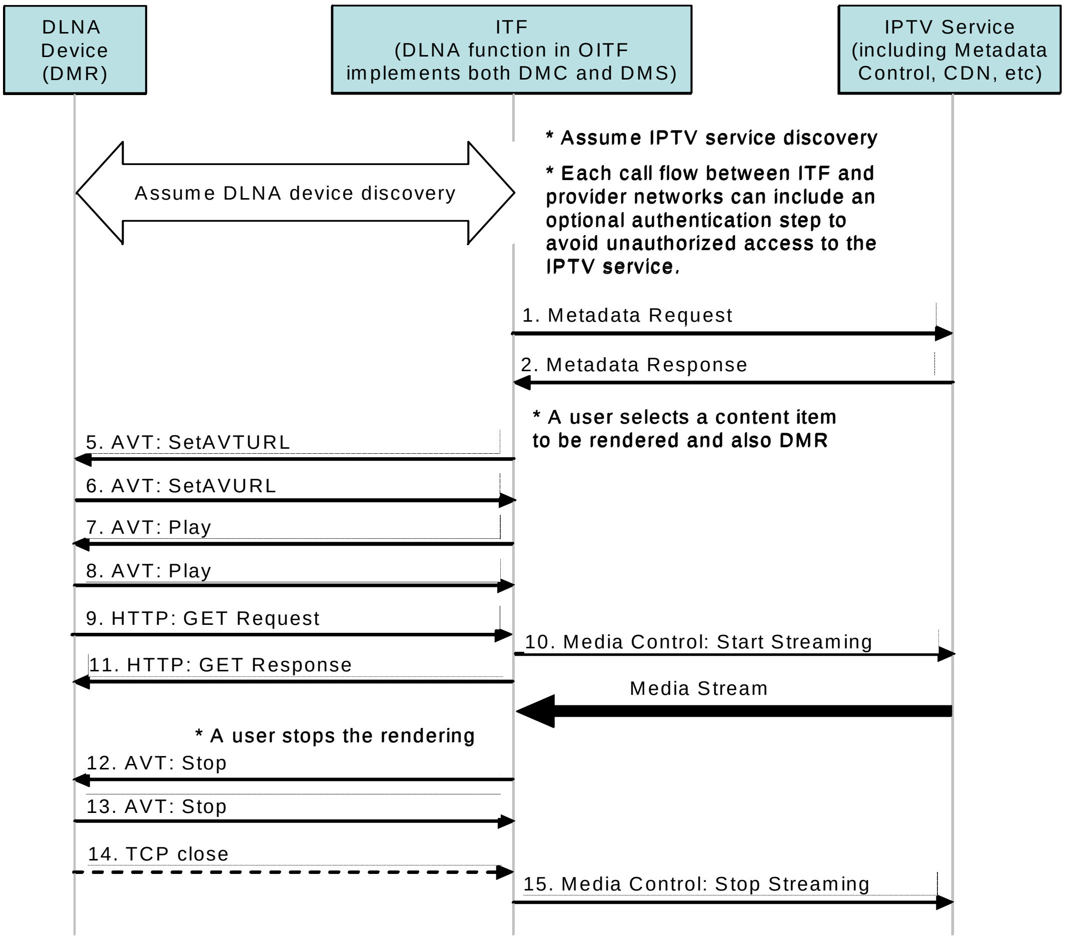

DLNA Device (DMR)
ITF (DLNA function in OITF implements both DMC and DMS)
IPTV Service (including Metadata Control, CDN, etc)
Assume DLNA device discovery
* Assume IPTV service discovery
* Each call flow between ITF and provider networks can include an optional authentication step to avoid unauthorized access to the IPTV service.
1. Metadata Request
2. Metadata Response
* A user selects a content item to be rendered and also DMR
5. AVT: SetAVTURL
6. AVT: SetAVURL
7. AVT: Play
8. AVT: Play
9. HTTP: GET Request
10. Media Control: Start Streaming
11. HTTP: GET Response
Media Stream
* A user stops the rendering
12. AVT: Stop
13. AVT: Stop
14. TCP close
15. Media Control: Stop Streaming

Figure 8-5: Signal flow for the 3 BOX system usage where the ITF acts as both a DMC and a DMS

8.4 2 BOX PUSH

The signal flow for the 2 BOX PUSH system usage shows the case where the ITF acts as a DLNA Push Controller (+UP+) and is the same as the 3 BOX PUSH system usage where the ITF acts as both a DMC and a DMS. In this system usage, a user operates the OITF which implements the DLNA push controller (+PU+), as shown in Figure 8-6.

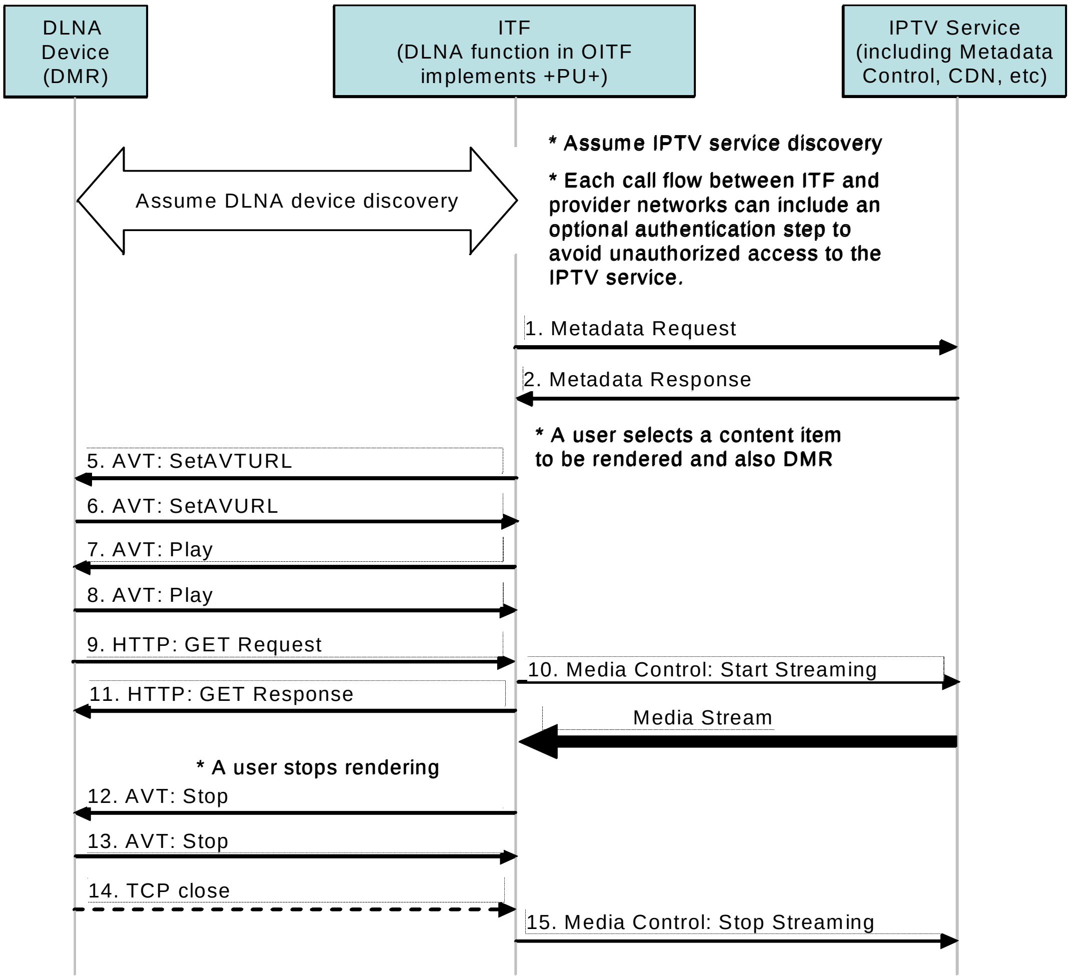

DLNA Device (DMR)
ITF (DLNA function in OITF implements +PU+)
IPTV Service (including Metadata Control, CDN, etc)
Assume DLNA device discovery
* Assume IPTV service discovery
* Each call flow between ITF and provider networks can include an optional authentication step to avoid unauthorized access to the IPTV service.
1. Metadata Request
2. Metadata Response
* A user selects a content item to be rendered and also DMR
5. AVT: SetAVTURL
6. AVT: SetAVURL
7. AVT: Play
8. AVT: Play
9. HTTP: GET Request
10. Media Control: Start Streaming
11. HTTP: GET Response
Media Stream
* A user stops rendering
12. AVT: Stop
13. AVT: Stop
14. TCP close
15. Media Control: Stop Streaming

Figure 8-6: Signal flow for the 2 BOX PUSH system usage where the ITF acts as a DNLA Push Controller

8.5 UPLOAD

Figure 8-7 shows the signal flow for the upload system usage where the ITF acts as a DLNA Upload Controller (+UP+). In this system usage, a user operates the OITF which implements DLNA Upload Controller (+UP+).

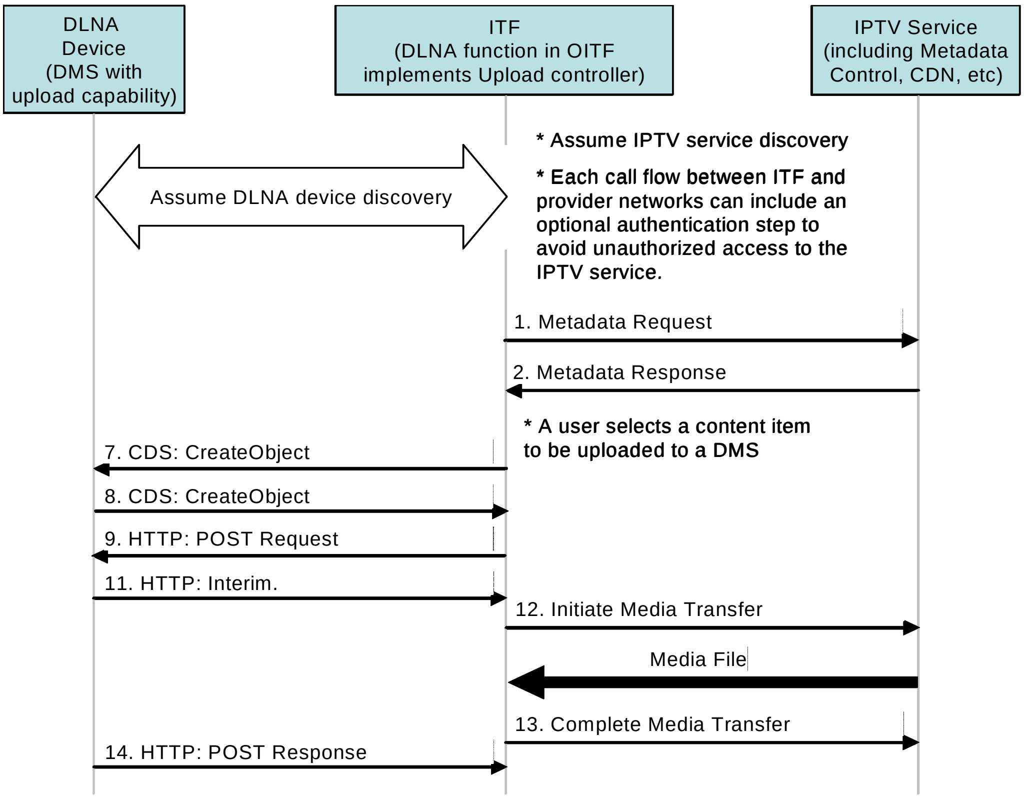

DLNA Device (DMS with upload capability)
ITF (DLNA function in OITF implements Upload controller)
IPTV Service (including Metadata Control, CDN, etc)
Assume DLNA device discovery
* Assume IPTV service discovery
* Each call flow between ITF and provider networks can include an optional authentication step to avoid unauthorized access to the IPTV service.
1. Metadata Request
2. Metadata Response
* A user selects a content item to be uploaded to a DMS
7. CDS: CreateObject
8. CDS: CreateObject
9. HTTP: POST Request
11. HTTP: Interim.
12. Initiate Media Transfer
Media File
13. Complete Media Transfer
14. HTTP: POST Response

Figure 8-7: Signal flow for a system usage where the ITF acts as a DNLA Upload Controller

Appendix A. Compliance of Architecture to the Requirements

Ref	Requirements Section	Compliance	Summary	Specific Requirement	Comments and clarification.
5	Service Requirements				
5.1	General	Compliant	General principles that have been taken into account in the architecture		
5.2	Provider Relationships	Compliant	Multiple IPTV service providers. Single Sign-on. IPTV Service provider with multiple SPP and access networks Simultaneous use of managed and unmanaged services.		
5.3	Service Categories				
5.3.1	Scheduled Content Service	Compliant	Scheduled content payment models. Manual configuration of service access? Channel change times.	[1-1170] [R1] The IPTV Solution shall make it possible for the user to configure (i.e. manually enter) the location of the IPTV resources providing the Scheduled Content Service. The location may be the service itself or a definition of the service and its offerings. [1-1180] [R1] Time delay in switching from one Scheduled Content Service to another should be minimized. The time should be no greater than 2 seconds and the goal should be <500ms.	No architectural implication. The R1 architecture should achieve the 2 sec channel change times assuming video GOP lengths are maintained at ~15 however the architecture does not include any architectural components designed to bring channel change times down to <500ms)
5.3.2	Content on Demand (CoD)				
5.3.2.1	Common Requirements	Compliant	General requirements including trick play and resume		
5.3.2.2	Streamed CoD Requirements	Compliant	Live streaming and progressive download	[1-1260] [R1] The IPTV Solution shall support the delivery of	No specific provider domain architectural support needed to support progressive

				CoD as live streaming and progressive download.	download.
5.3.2.3	Push CoD	Compliant	IPTV SP initiation to individuals and groups		
5.3.2.4	Deferred Download CoD	Compliant			
5.3.3	PVR				
5.3.3.1	Local PVR	Compliant	Scheduling via the user or via an application.	[1-1360] [R1] The IPTV Solution shall ensure that recordings which are made at the instigation of a Service Provider are not visible to other Service Providers.	Not an architectural requirement.
5.3.3.2	nPVR	Partially Compliant	Scheduling via the user or via an application		A description is needed in the architecture of how nPVR is supported including how the Content Storage database is used for nPVR recording and storing. Additional interfaces between the IPTV Control and content delivery are needed to control timer based recording of live multicast streams.
5.3.4	Time Shift	Compliant			Yes
5.3.5	Service and Content Navigation	Compliant			
5.3.5.1	Service Navigation	Compliant	Requirements refer to portal –		
5.3.5.2	Content Guide (CG	Partial Compliant for network implementation Compliant for implementation in OITF.		[1-1540] [R1] The IPTV Solution shall support filtering of Content Guide information to show different amounts of detail according to whether the content item is part of the subscription or not. [1-1550] [R1] The IPTV Solution shall support filtering of Content Guide information according to the rating of the item and the personal profile (including parental	Additional inter FE interfaces may be required.

				controls placed if any) of the user.	
5.3.6	User Notification Service	Compliant			
5.3.7	Advertising	Non Compliant		[1-1620] [R1] The IPTV Solution shall support mechanisms for the insertion of advertising graphics and video content in non-video (information) services. [1-1630] [R1] The IPTV Solution shall allow for the selection and presentation of advertising material on a regionalized basis. [1-1640] [R1] The IPTV Solution shall allow for the insertion of advertising material utilizing network located equipment. [1-1650] [R1] The IPTV Solution shall allow for the insertion of advertising material utilizing home network based equipment. [1-1660] [R1] The IPTV Solution shall allow advertising material containing textual and graphic items to be overlaid with transparency into video streams. [1-1670] [R1] The IPTV Solution shall allow advertising material containing textual and graphic items to be presented in a horizontal “ticker style” format with the video stream. NOTE: This format should consume less than 10% of the available vertical resolution. [1-1680] [R1] The IPTV Solution shall	Needs a review to determine whether all requirements can be implemented by embedded applications or network IPTV applications without new architectural components. VHO add insertion. needs a new component and interfaces in the network

				support mechanisms for the user to log (e.g. bookmark) individual advertisement information. [1-1690] [R1] The IPTV Solution shall support various advertising media such as video, audio, graphics, text.	
5.3.8	Communication Services				
5.3.8 .1	Caller ID	Compliant			The required asynchronous notification mechanism needs to be addressed.
5.3.8 .2	Presence	Compliant			The required asynchronous notification mechanism needs to be addressed.
5.3.8 .3	Messaging	Compliant			The required asynchronous notification mechanism needs to be addressed.
5.3.8 .4	Chatting	Compliant			The required asynchronous notification mechanism needs to be addressed.
5.4	Application Deployment and Execution				
5.4.1	General Requirements	Compliant			
5.4.2	Common Requirements	Compliant			
5.4.3	Requirements Specific to Browser Applications	Compliant			
5.4.4	Requirements Specific to Executable Applications				
5.4.4 .1	General Requirements	Compliant			
5.4.4 .2	Functional Requirements	Compliant			
5.4.4 .3	User Interface Requirements	Compliant			
5.4.5	Other Requirements	Compliant			
5.5	Security				
5.5.1	Access control				
5.5.1 .1	Application Security	Compliant		Specific Architectural support not required.	
5.5.2	Authentication				

5.5.2.1	User Authentication	Compliant			
5.5.2.2	Application Authentication	Compliant	No specific architectural support.		Protocols and application environment definition – no specific architectural additions needed.
5.5.3	Data Confidentiality	Compliant	No data export interface defined.	[1-2440] [R1] The operation of the IPTV Solution shall not require disclosure of information on each item of content being consumed by a user to any party other than the provider of each specific item of content. NOTE: Wider disclosure of information may be allowed either following consent by users or as a consequence of regulatory or legal requirements.	The note is not part of the requirement, as clarified by the Requirements WG.
5.5.4	Service and Content Protection / DRM	Compliant			
5.5.5	Communication Security	Compliant			
5.6	Remote Management	Compliant			
5.7	Registration	Compliant			No specific architectural support. These requirements are for the process of signing up for a subscription. Covered by O&M to service profile interfaces. O&M not including in the architecture.
5.8	Charging	Partially compliant		[1-2770] [R1] When the appropriate relationships and agreements are in place between the access network provider, IPTV Service Provider and SPP, the IPTV Solution shall support a mechanism for the SPP can to aggregate charging data with respect to usage of the access network and/or	IMS Service level charging is covered by existing IMS charging capabilities.

				IP connectivity services with charging data generated with respect to usage of Platform Provider services and the IPTV services of IPTV Service Providers.	
5.9	Accessibility	Compliant		[1-2830] [R1] The IPTV Solution shall include facilities to deliver services and content with accessibility enhancements to aid users with impaired vision or hearing. [1-2840] [R1] It shall be possible for the Service Provider to include additional service or content components that provide, for example a subtitle (closed caption) stream, or an additional descriptive audio stream. [1-2850] [R1] It shall be possible for the user to conveniently select the rendering of such auxiliary streams at the ITF. [1-2860] [R1] The IPTV Solution shall enable accessible user interfaces for IPTV services, e.g. for the handicapped or elderly.	No specific architectural support. Protocols issue
5.10	Profiles				
5.10.1	User Profiles	Compliant			
5.10.2	Network Resources	Compliant			
5.10.3	Content “Parental” Control	Compliant			
5.11	Service Portability	Compliant			
5.12	Home Network	Compliant			Access protocol translation not covered by architecture.
5.13	Protocols and Data Formats				

5.13.1	Content Formats	Compliant			
5.13.2	Transmission Protocols	Compliant			
5.13.3	Control Protocols				
5.13.4	Content Download Protocols	Compliant			
5.13.5	Metadata	Compliant			
5.14	Data Export	Non Compliant			No interface defined
5.15	Managed Network Specific Service Requirements				
5.15.1	Network Resources	Compliant			
5.16	Open Internet Specific Service Requirements	Compliant			
5.17	Hybrid Device Requirements	Compliant			

Table 6: Compliance to the Requirements

Appendix B. Proxy Description and GBA Single Sign-on (Informative)

This section introduces single-sign on architecture defined for IMS, and known as the Generic Bootstrap Architecture (GBA) [Ref 25], and the role the authentication proxy.

B.1 GBA Single Sign-on Architecture Description

Figure B-1 depicts the proposed GBA Single Sign-on architecture. This architecture capitalizes on the existing authentication schemes that are deployed to register an ITF to the network, and the shared secret between the ITF and certain network entities.

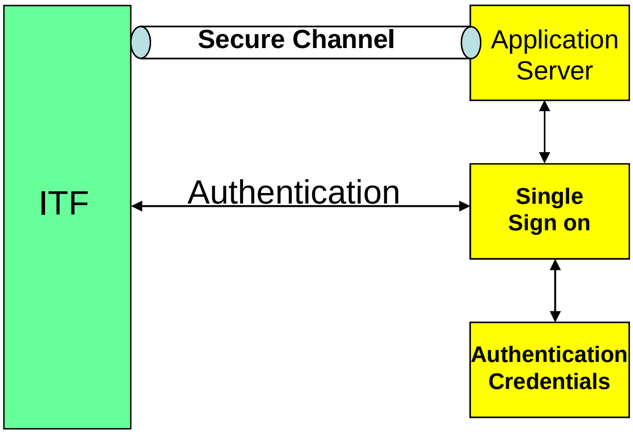


Figure B-1: GBA Single Sign-on Architecture

An ITF that desires to establish a secure channel with an Application Server (AS) before accessing the service must be able to acquire a key to share with the AS for securing its communication with that AS.

For that purpose, the ITF authenticates itself to a trusted node in the network dedicated for that purpose. This is the role of the GBA Single Sign-on function. Once successfully authenticated with the GBA Single Sign-on function, the ITF generates locally a master key that it uses to generate the key to be shared with the AS. The Single Sign-on FE performs the same procedure and generates the same master key. The procedure used to generate the key shall be known to the ITF and the GBA Single Sign-on function, and is based on existing standard mechanisms.

As previously stated, the master key generated in the ITF and the Single Sign-on node is used to generate the key to be shared with the AS. In order to allow the ITF to share separate keys with the different ASs with whom it wants to communicate, the AS URI can be used in the generation of the shared key in combination with the master key.

Later on, when the ITF attempts to activate the service, mutual authentication is required with the AS. Server certificates can be used by the ITF to authenticate the AS. Following that, a secure channel can be established. Once the secure channel is set up, the user can be authenticated by the AS using the shared key. The ITF uses the shared secret as a password, and the AS can fetch the same key from the GBA Single Sign-on function. Once mutual authentication is successfully concluded by the AS, it can verify if the user is authorized for the service. Obviously that step is skipped if the mutual authentication cannot be established. Service authorization is based on the service access information in the Subscription profile.

Figure B-2 depicts a call flow illustrating the above procedure:

1. The ITF authenticates itself with the GBA Single Sign-on function using the same credentials used in the IMS registration process

2. The ITF generates a master key locally and uses that key to generate separate keys for all ASs with whom it desires to communicate.

3. The GBA Single Sign-on function performs the same process.

4. The ITF establishes a secure channel with the AS using the AS’s public server certificate for that purpose.

5. The AS fetches the shared key for that user from the GBA Single Sign-on function.
6. The ITF then uses the shared key with the AS as its password to authenticate itself. The AS compares the received password with the one fetched from the GBA Single Sign-on function.
7. Mutual authentication is now completed and signalling exchange can start.

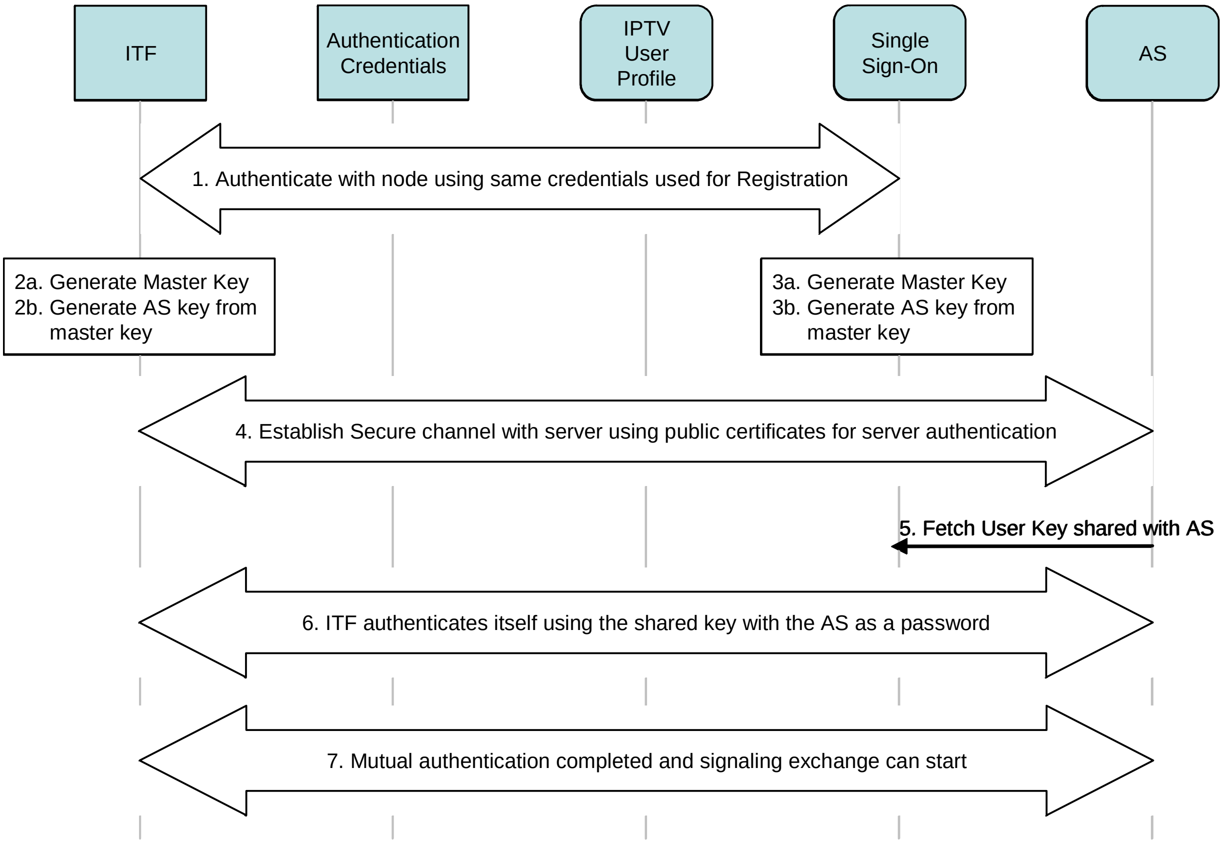

ITF
Authentication Credentials
IPTV User Profile
Single Sign-On
AS
1. Authenticate with node using same credentials used for Registration
2a. Generate Master Key
2b. Generate AS key from master key
3a. Generate Master Key
3b. Generate AS key from master key
4. Establish Secure channel with server using public certificates for server authentication
5. Fetch User Key shared with AS
6. ITF authenticates itself using the shared key with the AS as a password
7. Mutual authentication completed and signaling exchange can start

Figure B-2: GBA Single Sign-on call flow

B.2 Authentication Proxy and Service Access in a multi-AS Environment

The procedure presented in Figure B-2 shows that the AS must implement some specific procedures to be able to capitalize on the Single Sign-on procedure described above. This is not desirable since it implies that every AS must implement that scheme. In order to alleviate the need for the AS to have to cope with that, a new node, the Authentication Proxy node, is introduced in the network. Figure B-3 depicts such an architecture.

Within that architecture, the Authentication Proxy (AP) plays the same role depicted by the AS in the previous section. The advantage of such an approach are numerous: application servers don't need to do anything special in that regard, the ITF establishes a single secure channel with the AP and can use that to communicate with any AS later. Finally, any application server requiring such a scheme can be introduced in the network without any changes to existing architecture thus simplifying network deployment. Note that the AP is transparent to the ITF since the AP obtains the AS address through DNS lookup.

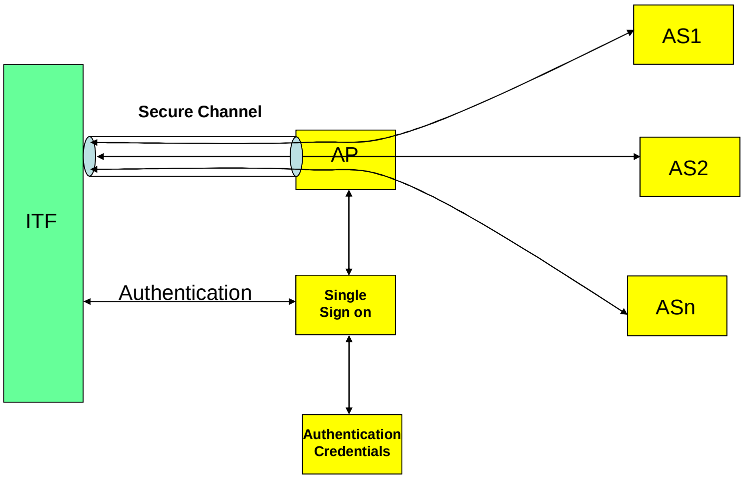


Figure B-3: Authentication Proxy and GBA Single Sign-on Architecture

Appendix C. Content Delivery Network Architecture description (informative)

C.1 General Description: CDN Architecture Overview

The CDN (Content Delivery Network) is a fundamental functionality in an IPTV CoD solution, since it allows the optimization of the network use through a distribution of the media servers in the physical network, and the optimization of the storage resources through a popularity-based distribution of the A/V content on the media servers. This usually results in having popular A/V content massively distributed on media servers at the edge of the network (as close as possible to the customer) while less popular content are distributed on an reduced number of media servers.

The following definitions and assumptions are used with regard to the CDN architecture:

- The term Video File corresponds to the Media of a movie stored on a CDF in a defined format.
- The term Content is a generic naming used in the present document to designate a video movie. It does not represent the physical media itself (which is the Video File). Content may be available in different Video File formats.
- The term Cluster corresponds to a logical association of one or more CDFs which share some resources (such as location, storage capacity).
- The term Cluster Controller (CC) corresponds to the function in charge of the management of the resources of the Cluster.
- A CDN is a set of CDFs/CCs/CDNC.
- One CDF belongs to only one Cluster at a time (1 Cluster : n CDF)
- One CC is responsible for the control of the CDFs associated with the Cluster (1 CC : n CDF) (This doesn't presume that CC function can not be redundant to improve service resilience)
- Both Cluster and ITF could have a location attribute which will allow calculating the 'Network distance' between the ITF and the Cluster. Other strategies could also be envisaged depending on the choice algorithm.
- Video Files available to customers are not necessarily distributed uniformly among the CDFs.
- A Video File may be present in some Clusters while absent in others.
- A Video File may be present in some CDFs within a given Cluster and absent in some other CDFs within the same Cluster.
- The ingestion and distribution of the Video Files among the CDFs is not in the scope of the contribution. However in some cases the distribution strategy and dynamic behaviour of content popularity can have a major impact on the choice of service and delivery setup.
- CCs are Managed by a CDNC (NB: This does not presume the number of instances of CDNC function across the CDN).

The hierarchical relationship between CDNCs/ CCs and CDF is shown in Figure C-1.

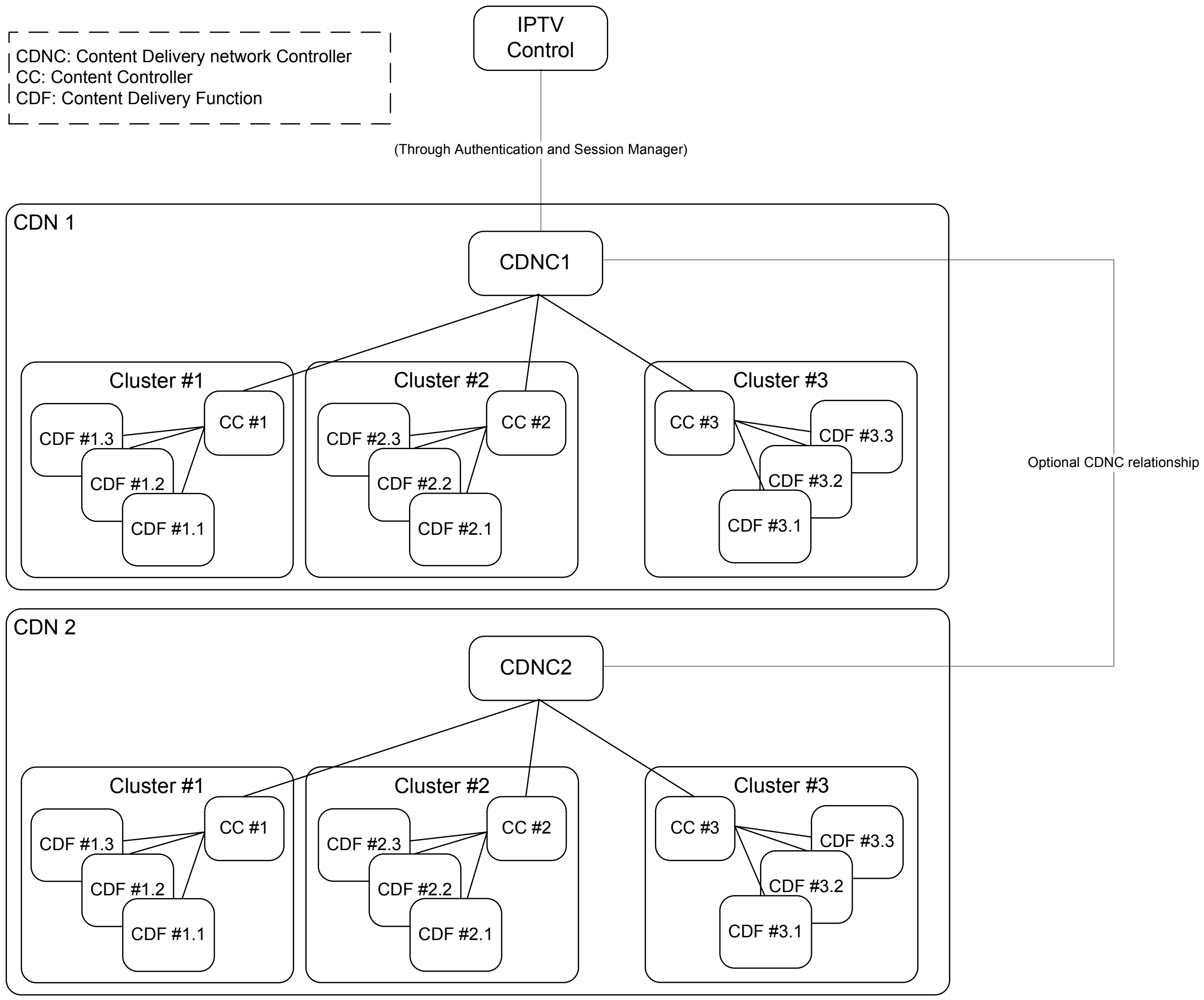


Figure C-1: Relationship between IPTVC/CDNC/CC/CDF

Two types of sessions are put in place to enable content delivery to the user:

- The Service Setup Session, which is used to setup an audiovisual service. It concerns the ITF, the Authentication and session management, the IPTV Control, the CDNC, the CC and the CDF. This session leads to the creation of a Content Delivery Session.
- The Content Delivery Session, which delivers the media from the CDF to the ITF. This session involves the ITF, the CC and the CDF. A Content Delivery Session is associated to a single Service Setup Session. This session is composed of :
  - A Content Delivery Session Control Plane: this allows the establishment of the Content Delivery Session and the control its progress.
  - A Content Delivery Session Transfer Plane: this allows the delivery of the media to the ITF.

Several Content Delivery Sessions can be created from the same Service Setup Session (for instance in order to take into account modifications in the course of the session). We consider here that these Content Delivery Sessions happen sequentially in time. Each Content Delivery Session contributes to the delivery of the media to the ITF.

Whenever the ITF or the CDF have to be re-selected (e.g. for service continuity), this causes to establish a new Content Delivery Session, If resource reservation is needed the service session needs to be updated. Please refer to section 6.4.2 for more information.

The IPTV Control, Authentication and session management and the CDNC can choose to stay informed with the Content Delivery Session progress and major events. They can change/teardown both sessions' parameters at any time, according to a defined policy.

C.2 Role of the CDN in the CoD service

The CDN operations, regarding the service setup session are organized in three sequential steps:

- CDNC selection
- CC selection
- CDF selection

C.2.1 CDNC selection

Two strategies can be applied while choosing the CDNC depending on the popularity of the content.

- If the content has a rather stable popularity, the choice of the CDNC can be performed directly by the IPTVC, and be considered as part of the Video file selection step. A stable popularity means the redistribution of the video files across the CDN is performed on a daily basis. This is the case of long, mainstream contents (e.g. movies). In order for the IPTVC to choose the CDNC it has to have the information that the video file is within the CDNC's stratum of the CDN. This corresponds to the call flows shown in section 6.4.1.
- If the content has a very dynamic popularity, the choice of the CDNC is left to a selection process performed across the CDN. A dynamic popularity means that the contents are redistributed across the CDN on an hourly basis (as an example). This is the case of short specialized contents, like music videos and user generated contents. Hence, the IPTVC does not need to keep up with all the file locations, and does not choose the CDNC, It forwards the aforementioned parameters to a default CDNC (for example) to trigger the decentralized selection process (as shown in Figure C-3). the right CDN controller's choice could be based on:
    - Video Content Selection Parameters
    - CDNC's organisation (Figure C-2 shows a few examples of such an organization)
    - Search and discovery algorithms (e.g., peer-to-peer algorithms, theme based, length based, etc.)

NOTE – it is required to have a mechanism to avoid a loop between CDNC, in order to implement this option

In both cases the choice of the target CDNC depends on a set of parameters generated by the IPTV controller such as:

- Applicable video files
- Access Network information
- ITF capabilities

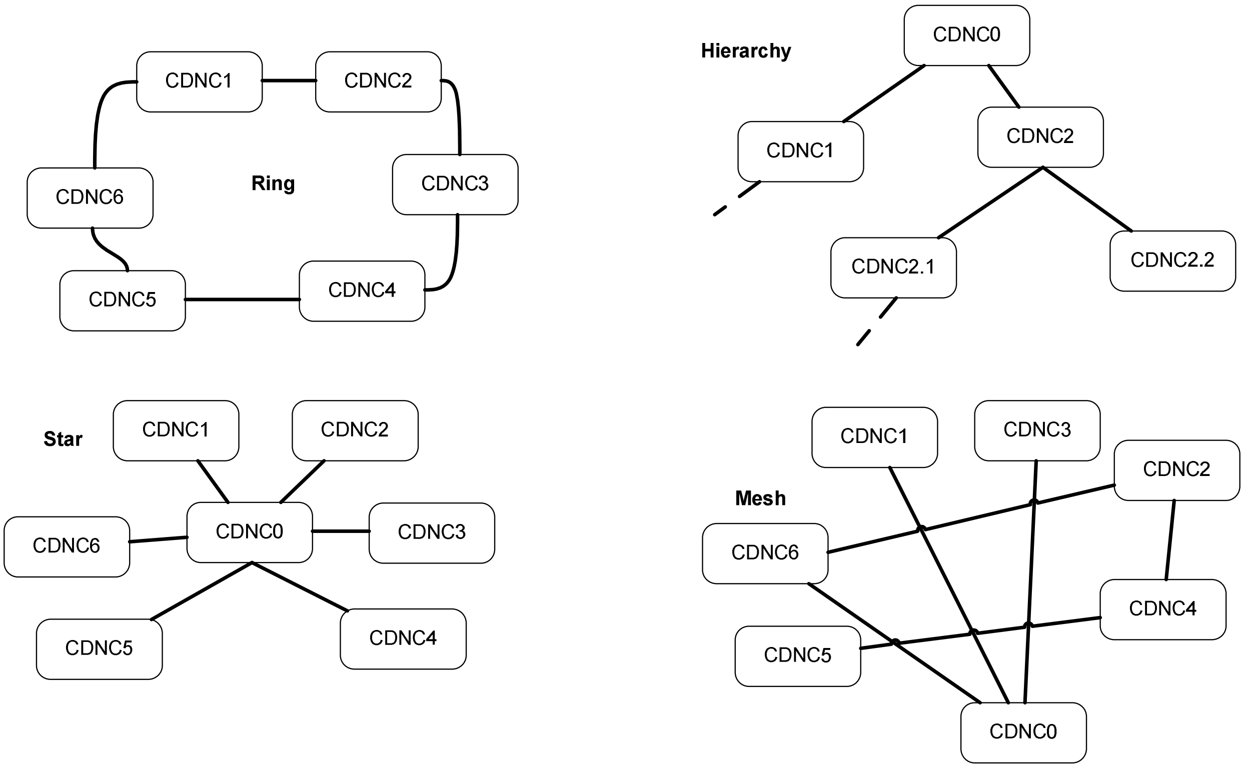


Figure C-2: CDNC organization examples

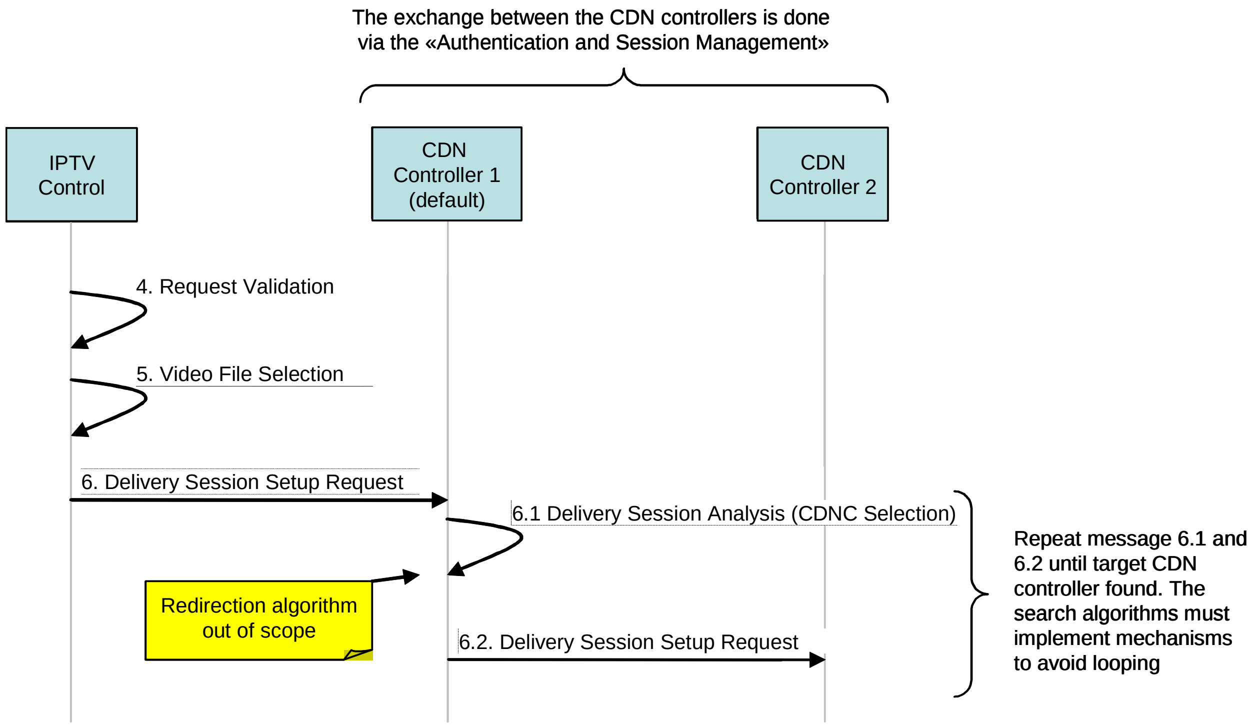

The exchange between the CDN controllers is done
via the «Authentication and Session Management»
IPTV Control
CDN Controller 1 (default)
CDN Controller 2
4. Request Validation
5. Video File Selection
6. Delivery Session Setup Request
6.1 Delivery Session Analysis (CDNC Selection)
Redirection algorithm out of scope
6.2. Delivery Session Setup Request
Repeat message 6.1 and 6.2 until target CDN controller found. The search algorithms must implement mechanisms to avoid looping

Figure C-3: The decentralized CDN controller choice option

C.2.2 CC selection

The chosen CDNC, shall choose, depending on the parameters generated by the IPTVC, the best cluster to Coordinate the content delivery session. The most important parameter in that choice could be the location and model of the ITF.

C.2.3 CDF selection

The chosen CC would then select the most appropriate Content Delivery Function, within the cluster, for sending the content to the user. The most important parameter in that choice would be the availability of the applicable files, and the load on the CDF's, visible only to the CC.

Once all the involved functions in the CDN are identified, the IPTVC is informed of the success and forwards a success message to the ITF, with the green light to proceed to the next step.

Appendix D. IMS User Identities (informative)

This section provides a brief overview of IMS User identities and how they can be used within the managed IPTV solution. For more information refer to TS 23.228 [Ref 15].

The examples and description within this section are based on IMS AKA authentication mechanisms described in section 6.3.2.1. This authentication mechanism requires one or more UICCs in the residential network.

The examples are not exhaustive.

D.1 Introduction

There are various identities that may be associated with a user of IP multimedia services described in the following subsection.

D.1.1 IMS Private User Identities - IMPI

Every user who wishes to participate in IMS-based communications services must be associated with one or more IMS Private User Identities (IMPI). An IMPI is assigned by the home network[2] operator at the time of subscription to IMS based services and used subsequently for Registration, Authorization, Administration, and Accounting purposes.

The Private User Identity is stored in the home network operator’s HSS as well as in a UICC (smart card) provided by the residential network operator to the subscriber, and is not accessible to the end user. In addition to storing the IMPI, the UICC also contains the security credentials (long term secret key) shared with the residential network operator and necessary for authentication.

The Private User Identity identifies the subscription, not the user. It is not used for routing of SIP messages. The Private User Identity is used to access, during Registration, the user's IMS-related subscription information (e.g. the security credentials needed for authentication) stored within the HSS.

The IMPI is authenticated using the security credentials stored in the UICC at the time of the registration (as well as during re-registration and de-registration).

The registrar in the residential network, the S-CSCF, obtains and stores the authenticated Private User Identity upon successful registration and deletes it when the UE is de-registered. The authenticated IMPI can be used by the S-CSCF to obtain from the HSS a list of the subscribed-to IMS services, so that subsequent attempts to communicate requiring these services can be authorized.

D.1.2 IMS Public User Identities - IMPU

An IMS subscription may support multiple end users. Each end user must be associated with one or more IMS Public User Identities (IMPU) for the purpose of IMS-based communications with services or other users. During registration, at least one IMPU is bound to the contact address (SIP URI containing the IP address) of the registering UE. This contact address serves as the point of contact for an end user associated with that IMPU for originating and terminating IMS sessions.

The IMPU takes the form of a SIP URI or a “Tel URI”. The residential network operator is responsible for the assignment of Public User Identities. The assignment of a human-friendly username for a SIP URI depends on the provisioning options offered by the operator.

The assignment of IMPUs associated with an IMPI to multiple end users is a matter for the owner of the subscription, and outside the scope of standardization.

Public User Identities are not authenticated by the network during IMS registration. Therefore, a communicating end user is not authenticated by the IMS network. This is not an issue for typical mobile person-to-person communications services,

[2] In telecommunications, the term “home network” refers to the network operator with whom a user has a subscription for services.

where there is usually a 1-to-1 relationship between the communicating end user and the holder of the subscription, and one can assume that an authenticated subscription implies an authenticated end user, but such a relationship cannot be assumed in the general case (multiple end-users associated with a single subscription).

Public User Identities may be used to identify the user's IMS profile within the HSS for example during mobile terminated session set-up.

D.2 Relationship of IMS Private and Public User Identities

The relationship of Public User Identities to Private User Identities, and the resulting relationship with an IMS subscription is shown in Figure D-1.

=

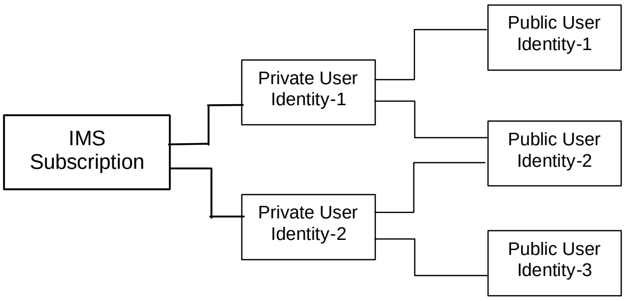


Figure D-1: Relationship of the Private User Identity and Public User Identities

A Public User Identity may be shared by multiple Private User Identities within the same IMS subscription.

Hence, a particular Public User Identity may be simultaneously registered from multiple UEs that use different Private User Identities and bound to different contact addresses.

D.3 Relationship of IMS Service Profiles to IMPIs/IMPUs

An IMS Service Profile is a collection of service and user related data as defined in 3GPP TS 29.228 [Ref 26]. It is possible to identify the Public User Identities of a user who is linked to the same service profile and has the exact same service configuration for each and every service (i.e. “alias” Public User Identities).

The IMS service profile is defined and maintained in the HSS and its scope is limited to IMS Core Network Subsystem. A Public User Identity is registered at a single S-CSCF. All Public User Identities of an IMS subscription are registered at the same S-CSCF. The service profile is downloaded from the HSS to the S-CSCF. Only one service profile can be associated with a Public User Identity at the S-CSCF at a given time. Multiple service profiles may be defined in the HSS for a subscription. Each Public User Identity is associated with one and only one service profile. Each service profile is associated with one or more Public User Identities.

The relationship for a shared Public User Identity with Private User Identities, and the resulting relationship with service profiles and IMS subscription, is depicted in Figure D-2.

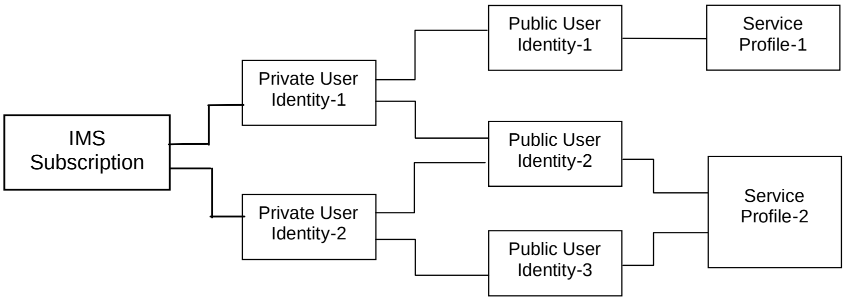


Figure D-2: Relationship of the Private User Identity and Public User Identities to Service Profiles

All Service Profiles of a user shall be stored in the same HSS, even if the user has one or more shared Public User Identities.

D.4 Identity Model Options in IMS-IPTV

To use IMS capabilities and allow personalization of the IPTV services and blending of IPTV and IMS services, subscribers must be assigned IMS public identities as per 3GPP principles and TS 23.228. [Ref 15]

Each IMS Public Identity associated with an IMS-IPTV subscription represents a user within the household. This identity is used when the user “logs on” to the ITF for personalized IPTV services using the specific IMPU assigned to them (i.e., registers with the IMS network). A user can have more than one IMS Public Identity if they so choose. How the user is assigned one or more IMPU(s) is out of scope of standardization, but normally this is done by the owner of the subscription (e.g., head of household) in some manner.

Where multiple public identities are associated with an IMPI, one of these identities serves as a default public identity and is not associated with a member of the household.

At power-up the default public identity associated with the IMPI is registered on successful authentication of the IMPI. Once the default identity successfully registers in IMS, the service profile associated with the default identity is available to all users within that IPTV subscription so long as they do not login with their own public identity. In this case their personal profile takes over after they have successfully registers their public identity in IMS.

The ISIM, or IMS Subscription Identity Module, contains the collection of parameters that are used for user identification (IMPUs), user authentication (long-term secret key shared between ISIM and home IMS network) and terminal configuration.

One ISIM application will host one IMPI and at least one IMPU.

There can be several ISIMs on one UICC, and they can also co-exist with other SIMs and USIMs

Multiple options are available for

- the number of IMPIs to be deployed within a house hold
- the number of IMS-IPTV subscriptions,
- how the public identities should be associated with the IMPIs and the IMS-IPTV subscriptions.

These options depend on a number of factors, including,

- the deployment scenario,
- the level of desired privacy and security within a household,
- the billing needs for the household,
- the number of devices in the household,

- the roaming needs of various members in the household.

The following sub- sections describe the main features of these options, including the pros and cons,

For the illustration of the options, it is assumed that members in a household are a mom, a dad and a son. Note that even though in the following sections the term UICC is used, the ISIM could as well be running in a software container.

Option 1: Shared UICC for the entire household

In this option, all household members share a single UICC. There are several sub-options in this option.

Option 1.1: All IMPUs are associated with a single IMPI

This is depicted in Figure D-3 below. In this sub-option, all IMPUs are associated with the same IMPI. There would be also a single IMS IPTV subscription for the entire household.

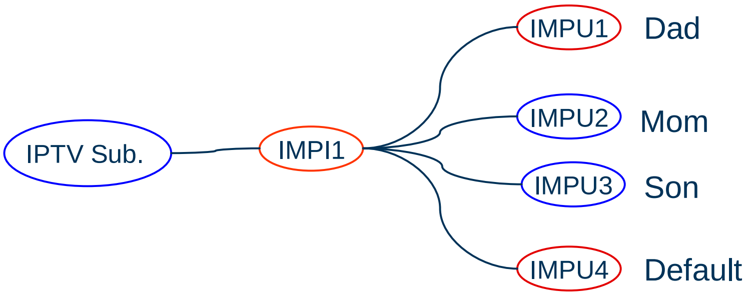


Figure D-3: All IMPUs associated with a single IMPI

Pros:

- No need to change UICC when a household member wants to register. Hence from a usability point of view, this is quite convenient

Cons:

- Any member of the household can use any one of the IMPUs at the time of registration, unless application support is provided that allows a particular user to login to the OITF prior to performing IMS registration using a particular IMPU

Given that this option requires means to prevent identity theft, it is more appropriate for a deployment that includes an IMS gateway (IG) that can house such an application and the UICC, provided that the LAN in the house is secure so that passwords cannot be stolen while being transferred from an OITF to the gateway.

Option 1.2: Each IMPU is associated with a Different IMPI

This is depicted in Figure D-4 below. In this sub-option, each member in the household will have a different IMPI. A UICC (or its software equivalent) hosts multiple ISIM applications, each one associated with one IMPI.

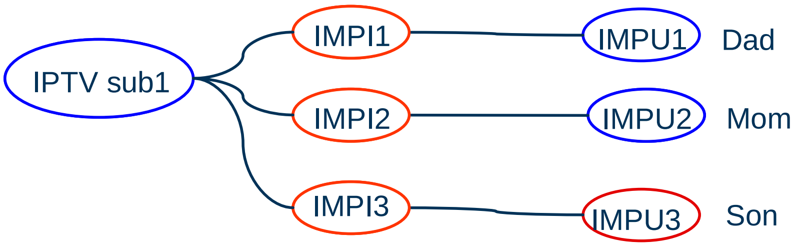


Figure D-4: 1:1 IMPU -IMPI relationship

Pros:

- No need to change UICC when a household member wants to register.
- Identity theft is not possible as each user has to individually “unlock” his ISIM application

Cons:

- The UICC will have to incorporate multiple ISIM applications, one for each IMPI. This is not common today as operators are accustomed to have a single application on a UICC. UICC vendors will have to support means to allow a user to select the ISIM he wants (pin unlocking or password)

Option 1.3: Hybrid of Options 1.1 & 1.2

This is depicted in Figure D-5 below. This sub-option essentially includes some household members who are associated with one IMPI, while others who are associated with a separate IMPI

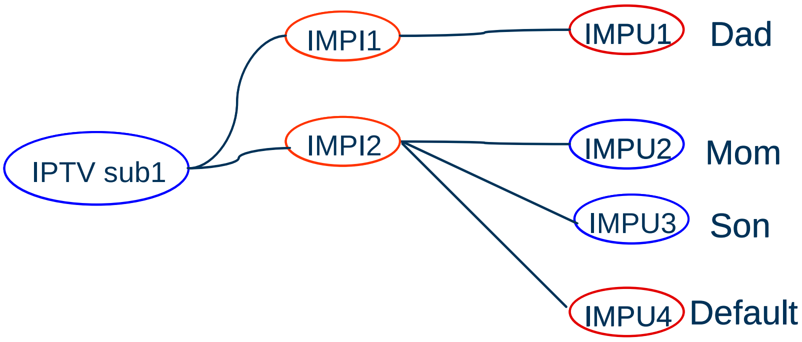


Figure D-5: Mixed IMPU -IMPI relationships

If the ISIM application including IMPI2 is selected then the default public identity will be the one to be registered by default at power-up. Following that, the son or the mom can IMS register their identities if they want to receive personalized service. If the ISIM application including IMPI1 is selected, then the dad’s public identity (IMPU1) will be registered by default.

Option 1.4: Household equipped with multiple OITFs.

If there are multiple OITFs in the house, and to enable the entire household to share a single UICC, then the household requires an IMS gateway (IG) for that purpose. Any household member can access the gateway from any OITF.

<u>Option 2: Multiple UICCs in the household with Single OITF</u>

In this option, each household member has a separate UICC (or its software equivalent). The household member can share the same IMS IPTV subscription or they can have different subscriptions.

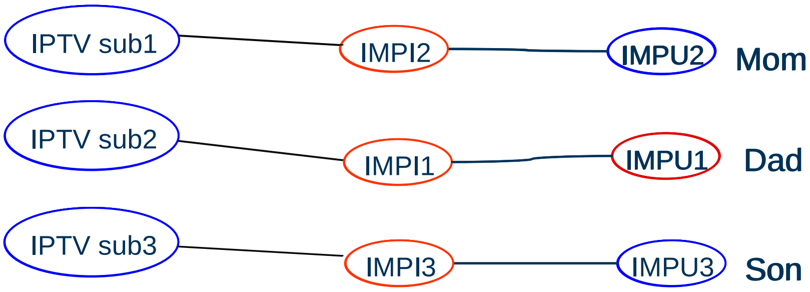


Figure D-6: Multiple UICCs

Pros:

- Complete privacy (no potential for any sharing)

- Aligned with today’s usage of UICC (one ISIM application per UICC)
- Flexible ISIM swapping between devices since every user has his own UICC.

Cons:

- Re-usability issues when it comes to device sharing in a household since

Appendix E. Resource and Admission Control for multicast (informative)

This Appendix gives a more detailed description of the Resource and Admission Control Transport and the relation with Multicast Delivery Function for an xDSL access network. It also gives more detailed information flows for multicast service support and QoS issues.

The solution described in this Appendix is purely functional. All the examples refer to xDSL.. The concepts described here, or similar ones, can be applied to other access technologies, but these are not described here for the sake of brevity.

E.1 Transport and Multicast Delivery Function description

The Network Operator's Transport and Multicast Delivery for multicast services support is typically composed by the following entities (as shown in the following picture):

- Transport Access Node (e.g. DSLAM): the access node
- Transport Remote Node (e.g. IP Edge or Feeder): the network element that resides at the boundary between core networks and access networks.
- Aggregation: the network which interconnects the Transport Access Node to the Transport Remote Node; the aggregation network between the Transport Access Node and the Transport Remote Node could include intermediate nodes which can be layer 2 or layer 3 based, depending on the Transport Access Node capabilities. A simplified configuration, including just Transport Access Node and Transport Remote Node, is used hereafter for the description of the resource reservation scenarios; however, this can be extended to more complex aggregation network configurations.

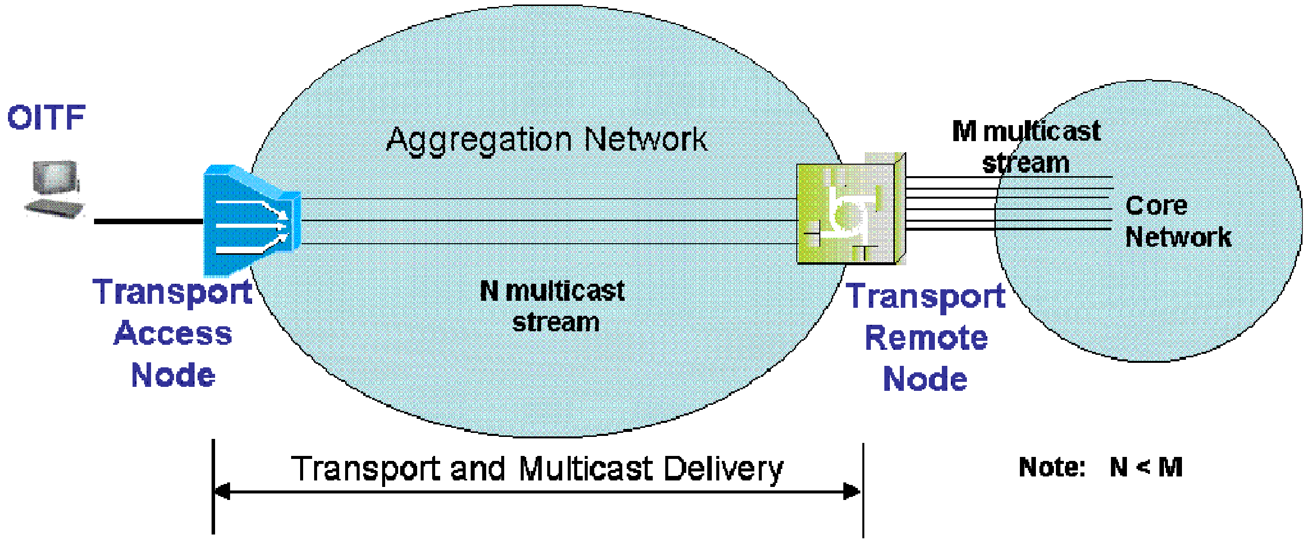


Figure E-1: Components of the Transport delivery network

Note that not every multicast channel is usually present at Transport Access Node (e.g. DSLAM), and the number of multicast streams that arrive at the Transport Access Node varies dynamically. Moreover, the network resources connecting the Transport Access Node to the Transport Remote Node (Aggregation or Metro Network) are limited, and a user could try to request a channel that at the moment is not already present at the Transport Access Node.

In a Layer 3 aggregation network, during multicast channel selection, the Transport Access Node terminates IGMP messages sent from the user (IGMP messages relating to the content delivery Session) and sends new IGMP or PIM messages to its neighbour nodes, the Transport Remote Node.

In a Layer 2 aggregation network, during multicast channel selection, the Transport Access Node snoops the IGMP messages sent from the user and forwards them upstream towards the Transport Remote Node.

In the following examples and call flows a layer 3 Transport Access Node using PIM for multicast signalling is considered, but the examples can easily be extended to other deployments.

With the context of this annex, it is assumed that there are no intermediate L2 or L3 nodes between the Transport Access node and the Transport Remote Node. This is a simplification that will be removed in subsequent revisions of this Annex.

When the ITF wishes to join a multicast channel with different QoS requirements (e.g. zapping from a SD to a HD channel) or if the stream for the new channel requested is not present in the Transport Access Node, in order to guarantee the needed bandwidth for the channel, an interaction between the Transport and Multicast Delivery Function and Admission Control entities is needed.

In particular at least 4 cases can be considered:

[1] If the stream of the channel requested by the user is already received by the Transport Access Node, and the authorized bandwidth in the last mile will not be exceeded by the addition of the bandwidth required by the channel to be viewed, the Transport Access Node terminates the IGMP join request, and streams the channel to the user;

[2] if the stream of the channel requested by the user is already received by the Transport Access Node, but the addition of the bandwidth required by the channel to be viewed exceeds the authorized bandwidth in the last mile, an interaction between the Transport Access Node and Admission Control entities is needed, to verify that there is enough bandwidth in the last mile and that it authorizes its use;

[3] if the stream of the channel requested by the user is not received by the Transport Access Node, and the authorized bandwidth in the last mile will not be exceeded by the addition of bandwidth required by the channel to be viewed, the Transport Access Node sends a PIM request to the Transport Remote Node to replicate the multicast stream to the Transport Access Node, if enough bandwidth is available in the aggregate network. The Transport Access Node in turn streams the channel to the user

[4] if the stream of the channel requested by the user is not received by the Transport Access Node , and the addition of the bandwidth required by the channel to be viewed will exceed the authorized bandwidth in the last mile:

- an interaction between the Transport Access Node and Admission Control entities is needed, to see if the required bandwidth can be made available in the last mile;

  If this is possible, then

  - The Transport Access Node sends a PIM request to the Transport Remote Node to replicate the multicast stream to the Transport Access Node, if enough bandwidth is available in the aggregate network. The Transport Access Node in turn streams the channel to the user

Section 5.4.1 describes the Resource and Admission Control (RAC) and Transport Processing Functions functional entities.

In the examples below, both the Transport Access Node and the Transport Remote Node comprise BTF, RCEF and A-RACF, but other deployments are allowed. The A-RACF in the Transport Access Node performs admission control for the access segment, while the A-RACF in the Transport Remote Node performs admission control for the aggregation segment.

The following section details some of the call flow related to the 4 cases considered above.

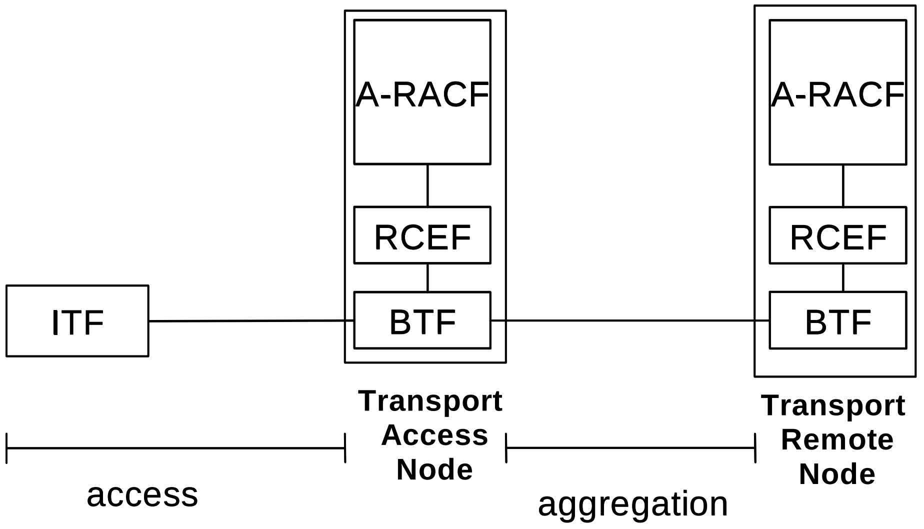


Figure E-2: Distribution of RAC functions between the various Transport nodes

E.2 ITF – Transport and Multicast Delivery call flow

In this section, a detailed information flow is presented, showing the interaction between ITF, Transport and Multicast Delivery and Admission Control functional entities.

The assumptions behind these scenarios are:

- The content to be accessed is not present in the Transport Access Node, but only in the Transport Remote Node, and the authorized bandwidth in the last mile will be exceeded by the addition of the channel to be viewed (case 4 considered in the previous section);
- The channel requested by the user is already received by Transport Access Node and the authorized bandwidth in the last mile does is exceeded by the addition of the channel to be viewed (case 2 considered in the previous section);
- Access Control List are pre-provisioned in the Transport Access Node to authorize the user request;
- The association between channels (or group of channels) and the bandwidth that they require is pre-provisioned in the Transport Access Node ;
- BTF + RCEF + Admission Control Function are present both in Transport Access Node and in the Transport Remote Node.
- There are no intermediate nodes between the Transport Access Node and Transport Remote Node

Other deployment configurations can be foreseen, as well as a more dynamic approach, based on a binding between the service authorization and the flow authorization. These cases are not covered in the following flows, but can be easily derived from them.

E.2.1 Channel requested is not present in the Transport Access Node and the authorized bandwidth in the last mile will not be exceeded (case 3)

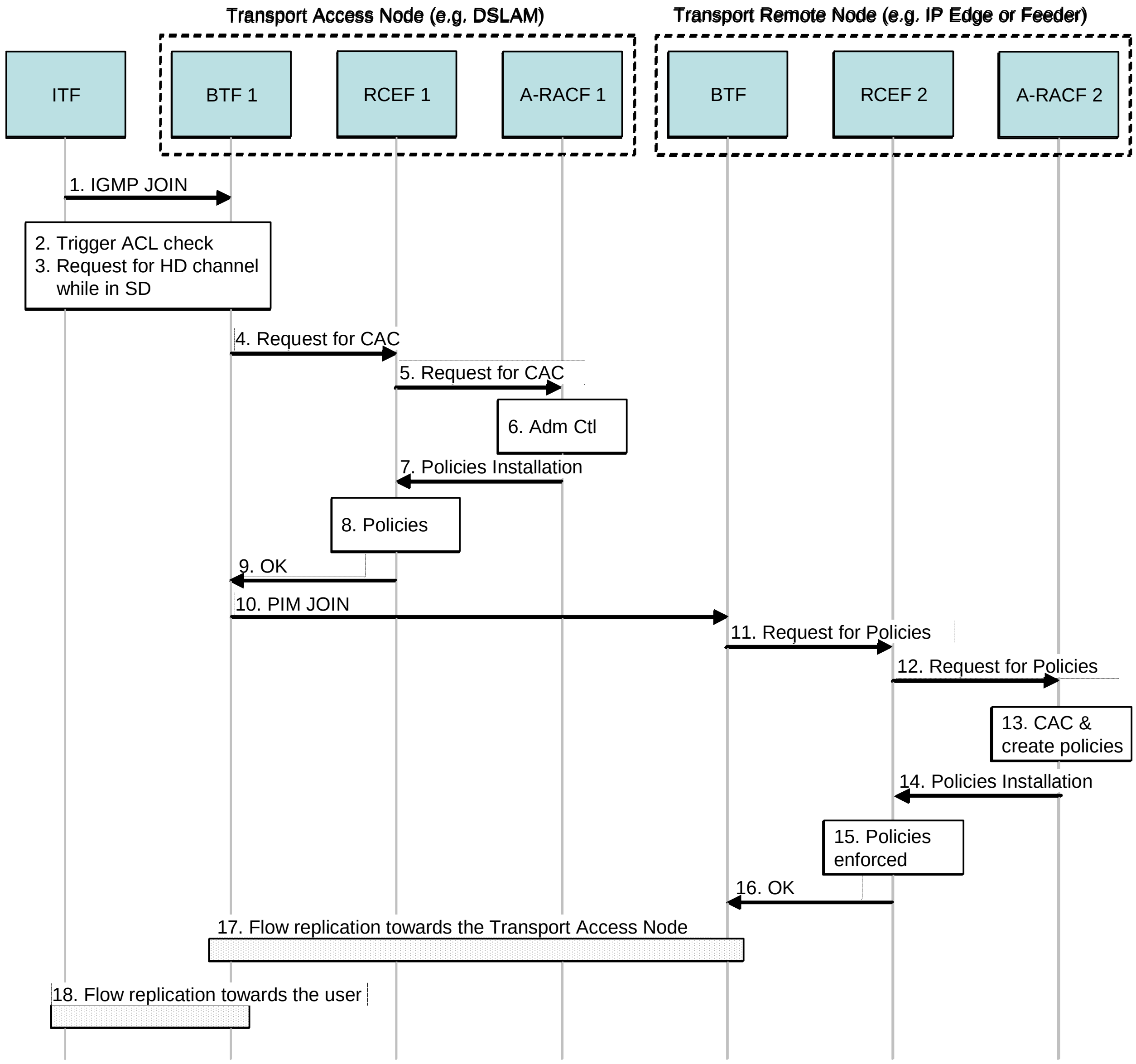

Transport Access Node (e.g. DSLAM)
Transport Remote Node (e.g. IP Edge or Feeder)
ITF
BTF 1
RCEF 1
A-RACF 1
BTF
RCEF 2
A-RACF 2
1. IGMP JOIN
2. Trigger ACL check
3. Request for HD channel while in SD
4. Request for CAC
5. Request for CAC
6. Adm Ctl
7. Policies Installation
8. Policies
9. OK
10. PIM JOIN
11. Request for Policies
12. Request for Policies
13. CAC & create policies
14. Policies Installation
15. Policies enforced
16. OK
17. Flow replication towards the Transport Access Node
18. Flow replication towards the user

Figure E-3: Call flow for case 3

The description of the steps is the following

1. The ITF requests an HD channel via IGMP Join
2. The IGMP message triggers the BTF in the Transport Access to authorize the request with the RCEF, where the pre-provisioned ACL are stored
3. Since the requested channel requires more bandwidth than the channel currently authorized, call admission control (CAC) is needed (
4. The BTF requests CAC towards the RCEF

5. The RCEF builds an admission control request and sends it to the A-RACF to obtain the authorizations on the network resources (previous service authorizations was made by IMS session)

6. The A-RACF in the Transport Access Node performs admission control on the access network and derives the traffic policies to be installed in the RCEF

7. The A-RACF sends the traffic policies to the RCEF

8. The RCEF enforces the traffic policies.

9. The RCEF answers positively to the BTF request

10. The BTF in the Transport Access Node sends a PIM join to the BTF in the Transport Remote Node, to be added to the multicast tree (PIM protocol is used to build a shared multicast distribution tree)

11. The BTF requests the needed policies from the RCEF

12. The RCEF forwards the request to the A-RACF

13. The A-RACF in the Transport Remote Node builds the required traffic policies to be installed in the RCEF. It is assumed as well that there is enough bandwidth in the aggregate network to send the stream to the Transport Access Node (14) The A-RACF sends the traffic policies to the RCEF

15. The RCEF enforces the traffic policies

16. The RCEF answers positively to the BTF request

17. The BTF in the Transport Remote Node starts to replicate the flow towards the Transport Access Node

18. The BTF in the Transport Access Node replicates the flow towards the User

E.2.2 Channel requested is present in the Transport Access Node and the authorized bandwidth in the last mile will be exceeded (case 2)

In this scenario the channel requested by the user is already received by Transport Access Node; the Transport Access Node terminates the IGMP, verifies that there is enough bandwidth in the last mile, and streams the channel to the user.

Steps 1 to 9 and step 18 from the figure for case 4 in section E.2.1 applies.

E.3 Linear TV and CoD unified view for reservation on Access segment

In this section, an example of information flow is provided to illustrate how an unified Linear TV and CoD Admission Control works with the architectural solution described in this Appendix.

The examples have the following assumptions:

- Linear TV and CoD service share the same transport resource in the last mile segment
- Linear TV and CoD service have different transport resources in the Aggregation segment
- The Linear TV channel requested by the user is already received by Transport Access Node (thus Admission Control for resources does not need to be performed in the aggregation segment) but the bandwidth in the last mile doesn't match the one needed by the channel to be viewed The following functional elements are involved (see Figure below):
- A-RACF 1 is an A-RACF deployed in the Transport Access Node.. A-RACF 1 performs Admission Control for the last mile segment for Linear TV only.
- RCEF 1 is deployed in the Transport Access Node

- BTF 1 is deployed in the Transport Access Node
- RCEF 2 is deployed in the Transport Remote Node
- BTF 2 is deployed in the Transport Remote Node
- A-RACF 0 is an A-RACF performing Admission Control for CoD in the Aggregation Segment and in the last mile segment. It is further handling Admission Control for Linear TV in the last mile segment through delegating an Admission Control budget to A-RACF 1. A-RACF 0 is hence aware of resource reservations in both the Aggregation and last mile segments.

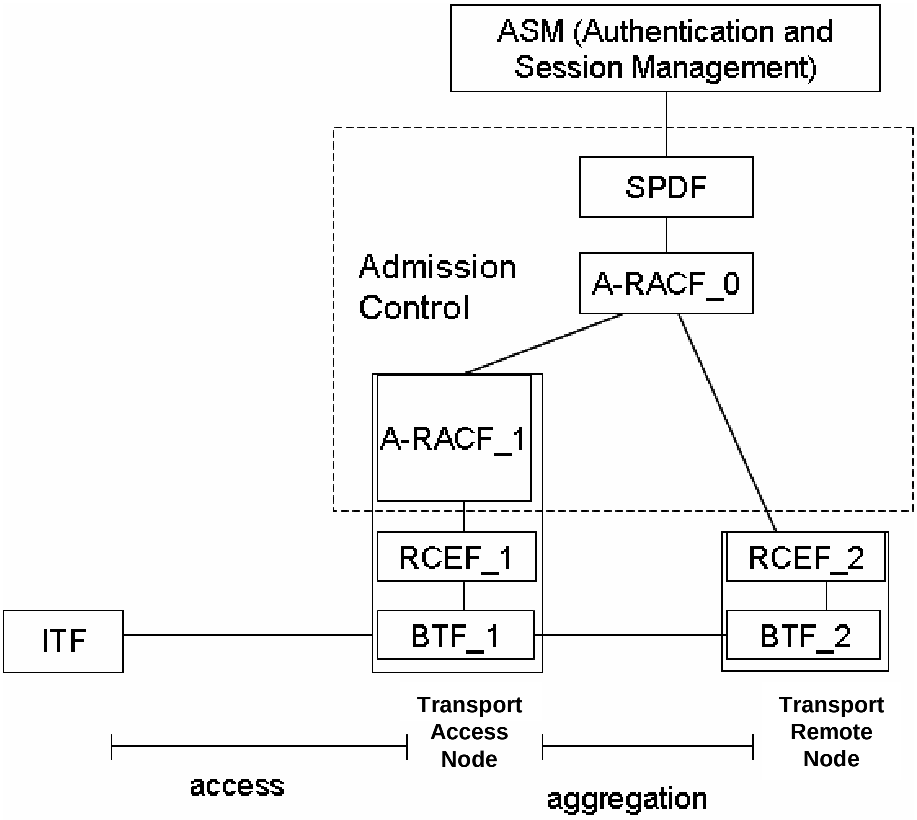


Figure E-4: Functions needed for a unified treatment of resource and admission control across access and aggregation networks

The Information flow for delivering both Linear TV and CoD comprises 3 phases:

1. Linear TV Session Initiation
2. CoD Session request and delivery
3. Linear TV delivery

E.3.1 Linear TV Session Initiation

In this phase, after receiving the user request, an admission control budget is installed in A-RACF_1 for Linear TV.

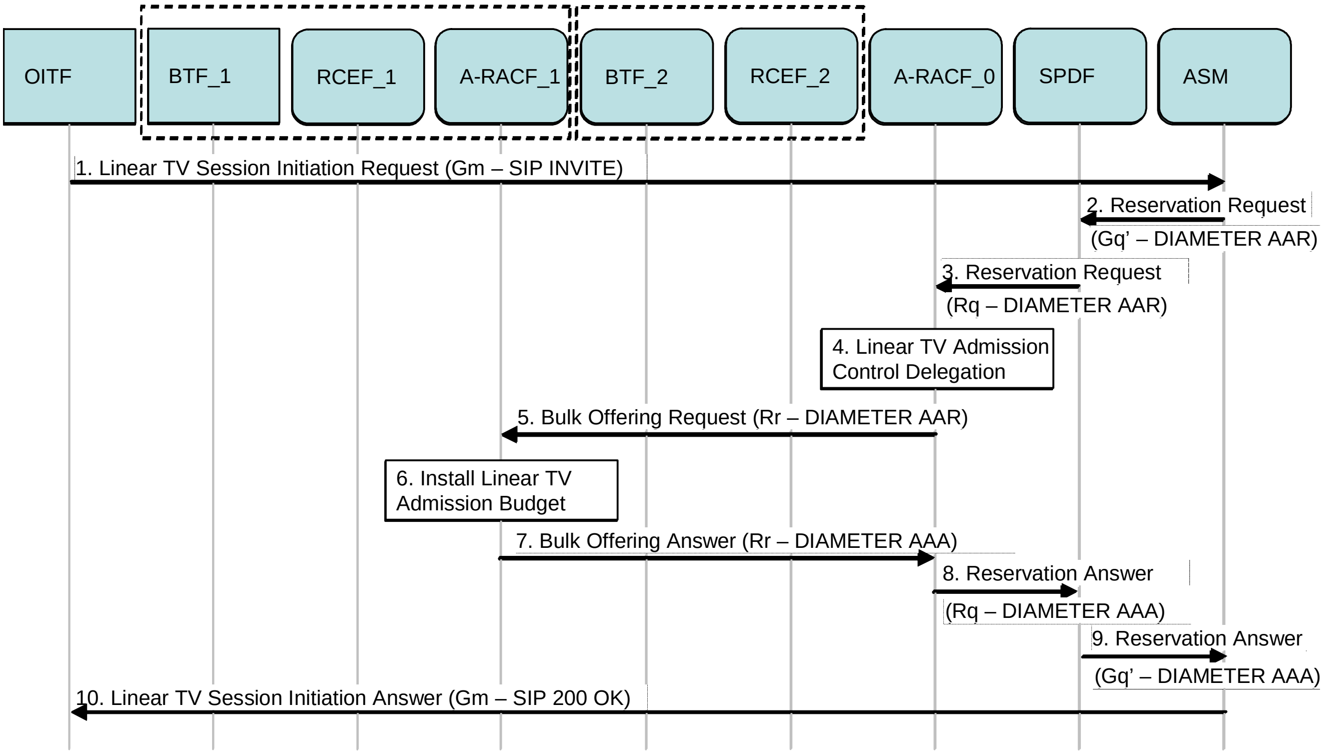

OITF
BTF_1
RCEF_1
A-RACF_1
BTF_2
RCEF_2
A-RACF_0
SPDF
ASM
1. Linear TV Session Initiation Request (Gm – SIP INVITE)
2. Reservation Request
(Gq' – DIAMETER AAR)
3. Reservation Request
(Rq – DIAMETER AAR)
4. Linear TV Admission Control Delegation
5. Bulk Offering Request (Rr – DIAMETER AAR)
6. Install Linear TV Admission Budget
7. Bulk Offering Answer (Rr – DIAMETER AAA)
8. Reservation Answer
(Rq – DIAMETER AAA)
9. Reservation Answer
(Gq' – DIAMETER AAA)
10. Linear TV Session Initiation Answer (Gm – SIP 200 OK)

Figure E-5: Admission control for Linear TV

1. The user requests access to Linear TV

2-3. Reservation request

4-7. A-RACF_0 installs a bandwidth budget in A-RACF_1

8-9. Reservation answers

10. Answer to the user request

E.3.2 CoD Session request and delivery

In this phase, a CoD request is received and A-RACF_0 does not have sufficient resources to fulfil the request in the last mile segment. It asks the A-RACF_1 for the needed resources which can be done by reducing its Linear TV budget provided that the bandwidth currently consumed by linear TV is below the admission control budget.

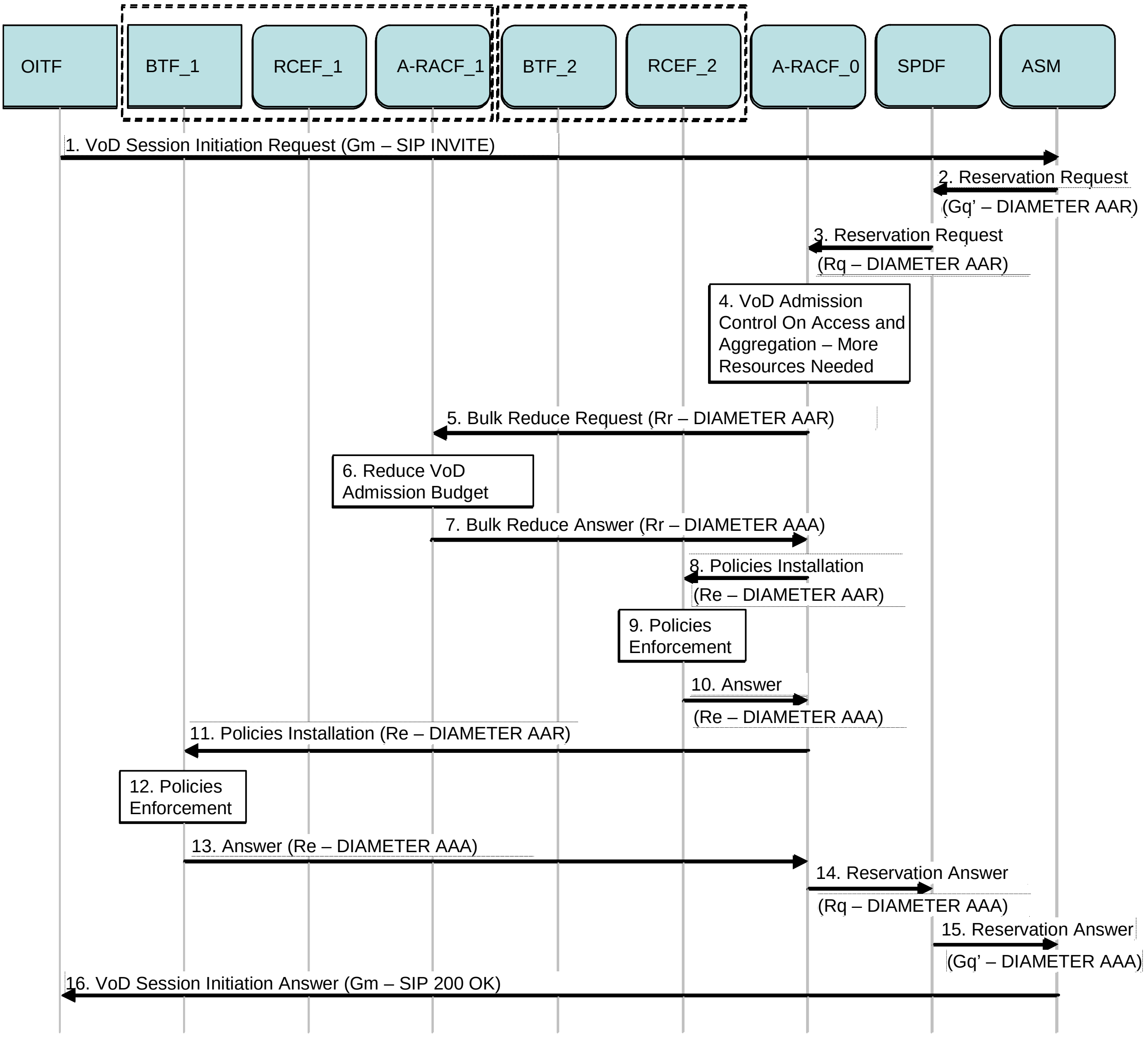

OITF
BTF_1
RCEF_1
A-RACF_1
BTF_2
RCEF_2
A-RACF_0
SPDF
ASM
1. VoD Session Initiation Request (Gm – SIP INVITE)
2. Reservation Request (Gq' – DIAMETER AAR)
3. Reservation Request (Rq – DIAMETER AAR)
4. VoD Admission Control On Access and Aggregation – More Resources Needed
5. Bulk Reduce Request (Rr – DIAMETER AAR)
6. Reduce VoD Admission Budget
7. Bulk Reduce Answer (Rr – DIAMETER AAA)
8. Policies Installation (Re – DIAMETER AAR)
9. Policies Enforcement
10. Answer (Re – DIAMETER AAA)
11. Policies Installation (Re – DIAMETER AAR)
12. Policies Enforcement
13. Answer (Re – DIAMETER AAA)
14. Reservation Answer (Rq – DIAMETER AAA)
15. Reservation Answer (Gq' – DIAMETER AAA)
16. VoD Session Initiation Answer (Gm – SIP 200 OK)

Figure E-6: Resource and admission control for VoD

1. The user requests access to CoD. A session setup request is propagated in the control plane.

2-3. A Reservation Request is sent to the A-RACF_0

4-7. A-RACF_0 requests the needed bandwidth from A-RACF_1. These steps are optional and depend on the capabilities of the A-RACF_0.

8-13. Policies related to the new linear TV budget and the unicast flow are installed, as appropriate, in the RCEFs

14-15. Reservation answers

16. Answer to user request

E.3.3 Linear TV delivery

In this phase the user accesses Linear TV and tries to view a channel that requests a higher bandwidth; A-RACF_1 has finished its Linear TV budget and asks for an increase to A-RACF_0.

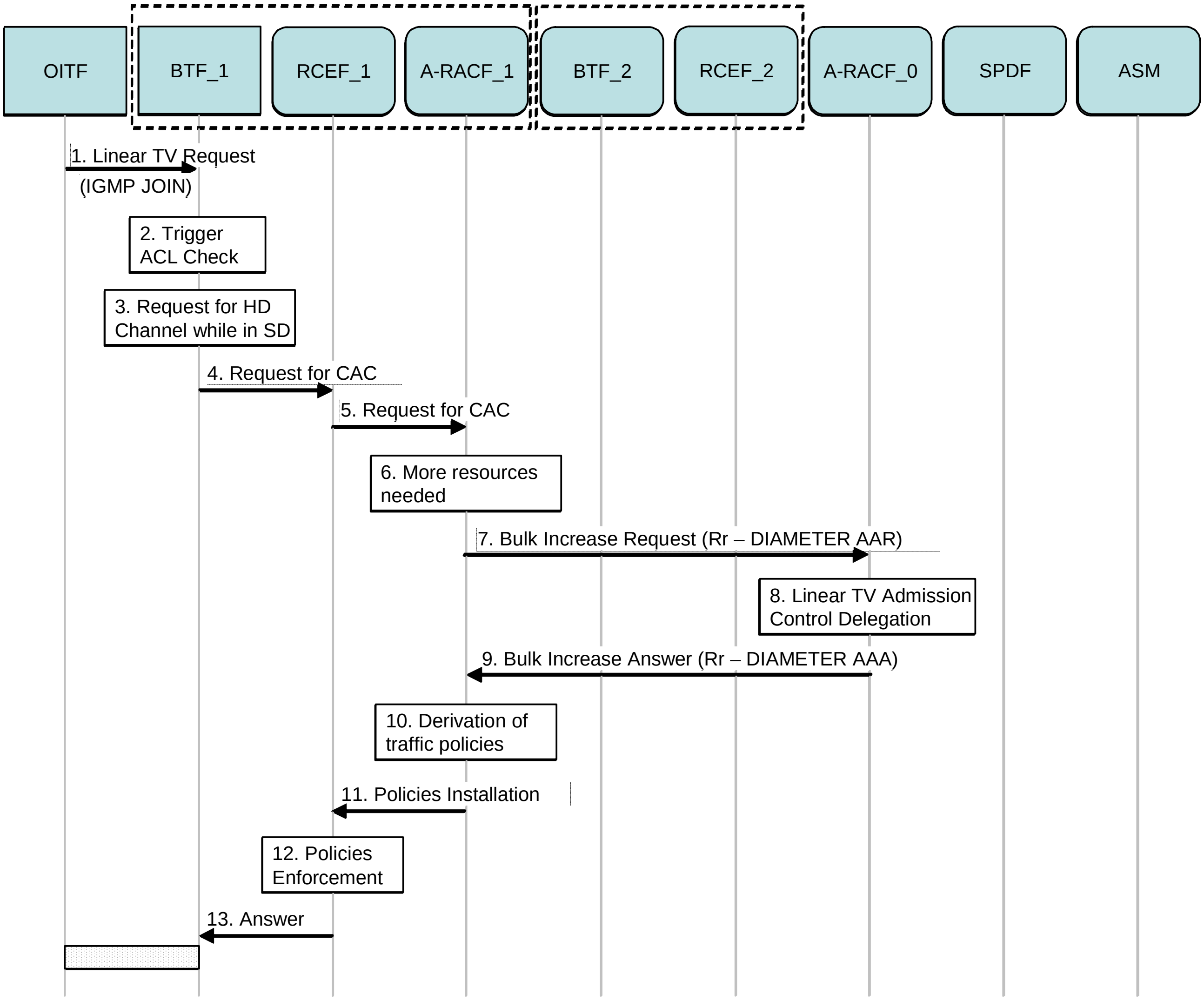

OITF
BTF_1
RCEF_1
A-RACF_1
BTF_2
RCEF_2
A-RACF_0
SPDF
ASM
1. Linear TV Request
(IGMP JOIN)
2. Trigger ACL Check
3. Request for HD Channel while in SD
4. Request for CAC
5. Request for CAC
6. More resources needed
7. Bulk Increase Request (Rr – DIAMETER AAR)
8. Linear TV Admission Control Delegation
9. Bulk Increase Answer (Rr – DIAMETER AAA)
10. Derivation of traffic policies
11. Policies Installation
12. Policies Enforcement
13. Answer

Figure E-7: Resource and admission control for linear TV with higher bandwidth requirement

1. User requests channel via IGMP

2. The IGMP message triggers the check of the ACL to authorize the request

3. Since the requested channel requires more bandwidth than the channel currently accessed, CAC is needed (call admission control)

4-5. CAC Request

6-9. Bandwidth not sufficient: request to A-RACF_0 for bandwidth increase

10-12. Installation of Policies.

13. Answer and Linear TV flow delivery

Appendix F. Change History (Informative)

Date	Version	Change
2008-01-15	1.1	Approved