Open IPTV Forum – Functional Architecture – V 1.0

Working Draft 20 – 09 -2007

This document is considered stable and is not expected to be modified for Release 1 except for those sections marked “under review”

Open IPTV Forum

Open IPTV Forum

Postal address

Open IPTV Forum support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 43 92
Fax: +33 4 92 94 43 42

Internet
http://www.openiptvforum.org

Disclaimer

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

Copyright Notification

Content

Figures

Tables

INTELLECTUAL PROPERTY RIGHTS

No guarantee can be given as to the existence of IPRs which are, or may be, or may become, essential to the present document.

FOREWORD

This document has been produced by the Open IPTV Forum.

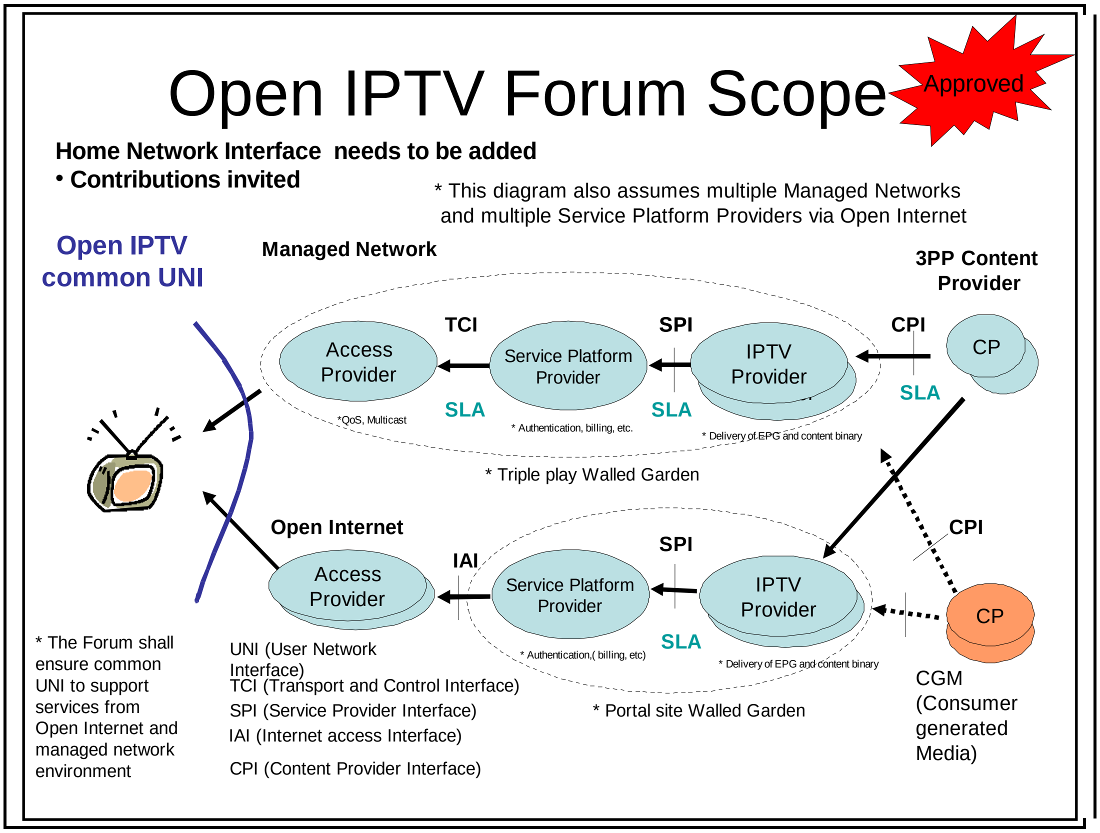
INTRODUCTION

This document describes the functional architecture as part of the Open IPTV Forum Release 1 specifications.

1. Scope (Informative)

The Open IPTV Forum was set up to develop 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.

In that respect, 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 0-1 .


Open IPTV Forum Scope

Home Network Interface needs to be added

• Contributions invited

* This diagram also assumes multiple Managed Networks and multiple Service Platform Providers via Open Internet

* 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)

Figure 0-1: 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

[Ref 1]	DSL Forum TR 69
[Ref 2]	3GPP Reference points
[Ref 3]	DLNA Guide Lines
[Ref 4]	CEA-2014
[Ref 5]	DVB-IP Blue Book
[Ref 6]	Ethernet Priority
[Ref 7]	DIFFSERVE
[Ref 8]	802.11
[Ref 9]	IGMP Snooping
[Ref 10]	IGMP Proxy
[Ref 11]	IGMP
[Ref 12]	PIM
[Ref 13]	TISPAN RACS
[Ref 14]	DVB BCG
[Ref 15]	RTCP
[Ref 16]	IMS Identity TS23 228
[Ref 17]	HTTP Digest Authentication RFC 2617
[Ref 18]	IMS Authentication TS 33 203
[Ref 19]	TISPAN HTTP Digest
[Ref 20]	RTSP
[Ref 21]	E164
[Ref 22]	IETF SIP RFC 3261
[Ref 23]	OMA “Instant Messaging using SIMPLE” (OMA-ERP-SIMPLE_IM-V1_0-20070816-C
[Ref 24]	ECMA Script
[Ref 25]	OMA “Presence SIMPLE Specification” (OMA-ERP-Presence_SIMPLE-V1_0_1-20061128-A)
[Ref 26]	IMS GBA
[Ref 27]	IMS Profiles TS 29 228
[Ref 28]	Diameter

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 by the Access Provider 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 Content on Schedule and Content on Demand, allowing a User to navigate, select, and discover content by time, title, channel, genre, etc.
Content on Demand (CoD)	An IPTV service where the play-out of the content is controlled by the end user.
Content Protection	Means to protect contents from unauthorized usage during its complete lifetime; it may involve usages such as re-distribution, recording, playback, duplication etc.; Content protection is enabled for encrypted content through the use of appropriate rules or rights.
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.
Residential Network	Residential consumer network.
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 Platform Provider	Entity that 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.
IPTV Service Provider	Entity that offers IPTV Services and which has a contractual relationship with the Subscriber.
IPTV Solution	Defined by the Forum Specification.
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 Service Provider to pre-load CoD).
nPVR	Provision of PVR functionality whereby the content is stored in the 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 Service Provider. The user has no direct control of what content is downloaded; however the Service Provider may make the choice based on user preferences and habits. Content is available for direct consumption after the user selection is confirmed.

Service Content and applications provided by Service Platform Providers and Service Providers.

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 with a Service Provider for the consumption of certain services.

Subscriber Profile Subscription information associated with an account.

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 Subscription information associated with a specific User, e.g., viewing preferences.

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**
DAE	**Declarative Application Environment**
DA-DLE	**Downloadable Application – Decrarative Language Environment**
DA-PLE	**Downloadable Application – Procedural Language Environment**
DLNA	**Digital Living Network Alliance**
DLNA DMS	**DLNA Digital Media Server**
DMP	**Digital Media Player**
DOS	**Denial of Service**
DRM	**Digital Rights Management**
DSCP	**DIFFServ Code Point**
DTT	**Digital Terrestrial Television**
DVB-IP	**Digital Video Broadcasting Internet Protocol**
ECMA	**Ecma International - European association for standardizing information and communication systems**
EPG	**Electronic Program Guide**
FE	**Functional Entity**
GENA	**General Event Notification Architecture**
GPON	**Gigabit Ethernet Passive Optical Network**
GUI	**Graphical User Interface**
HD	**High Definition**
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**
IPTV	**Internet Protocol Television**
ISIM	**IMS Subscriber Identity Module**
ITF	**IPTV Terminal Function**
M/C-U/C	**Multicast to Unicast**
LAN	**Local Area Network**
MAC	**Message Authentication Code**
MSRP	**Message Session Relay Protocol**

NAT	**Network Address Translation**
nPVR	**Network Personal Video Recorder**
OMA	**Open Mobile Alliance**
OITF	**Open IPTV Terminal Function**
QoS	**Quality of Service**
P2P	**Peer-to-Peer**
PC	**Personal Computer**
PLMN	**Public Land Mobile Network**
POTS	**Telephone 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**
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**
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 4.2-1.

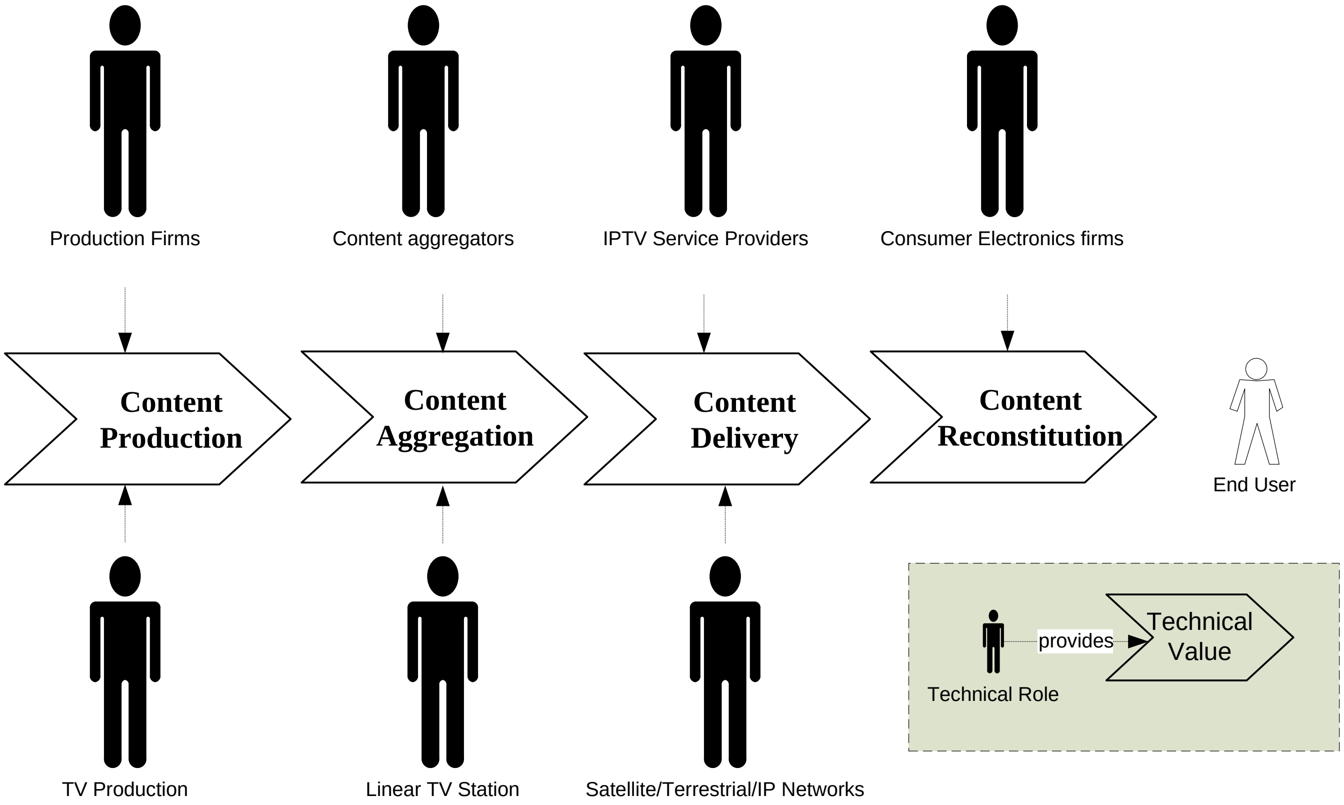


Figure 4.2-1: Content Value Chain

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 catalog 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 content services delivered over an end-to-end managed network. The end user can access content that is made available by the managed network.
- The Unmanaged Model: concerns access to and delivery of content services conforming to Open IPTV Forum specifications delivered over 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 Access 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 Access Provider to the consumer domain.

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

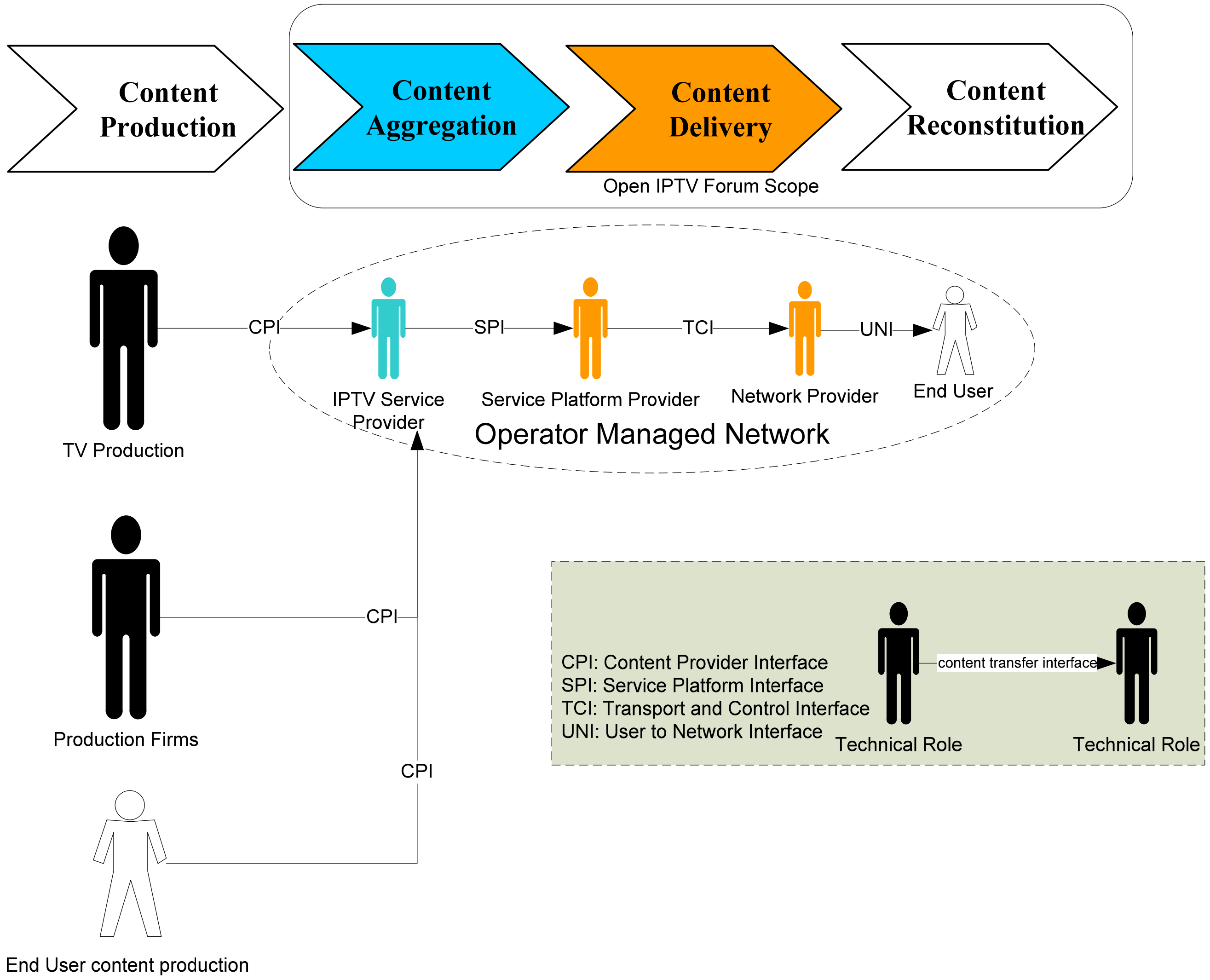


Figure 4.2-2: Managed Model technical roles and content transfer interfaces

4.2.2 Unmanaged Model

The Unmanaged model has the same set of technical roles as that of the managed model (See Figure 4.2-3), 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 access 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.

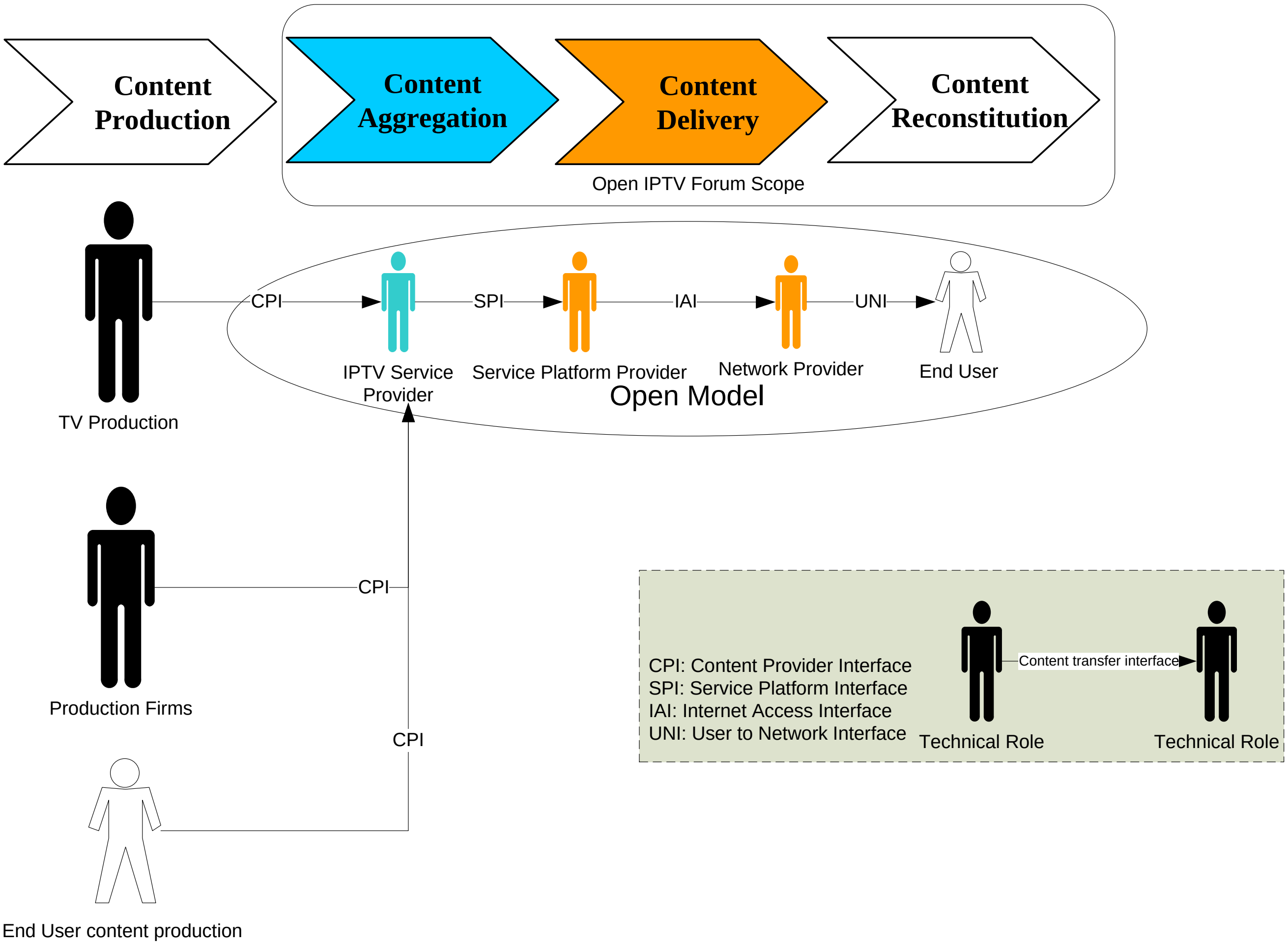


Figure 4.2-3 : Unmanaged Model technical roles and content transfer interfaces

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 6.1-1 shows the UNI interface between the Consumer Domain and the Network Provider, Service Platform Provider and IPTV Service Provider 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.

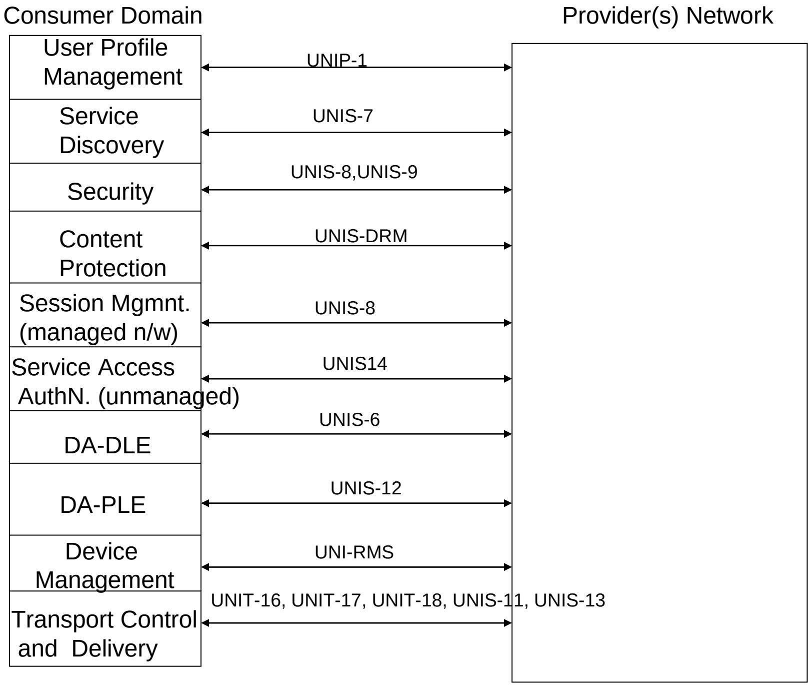


Figure 5.1-1: Mapping Functional Entities to UNI Reference Points

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 fulfill the desired features.

5.2 The Provider(s) Network Architecture

Figure 6.2-1 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.

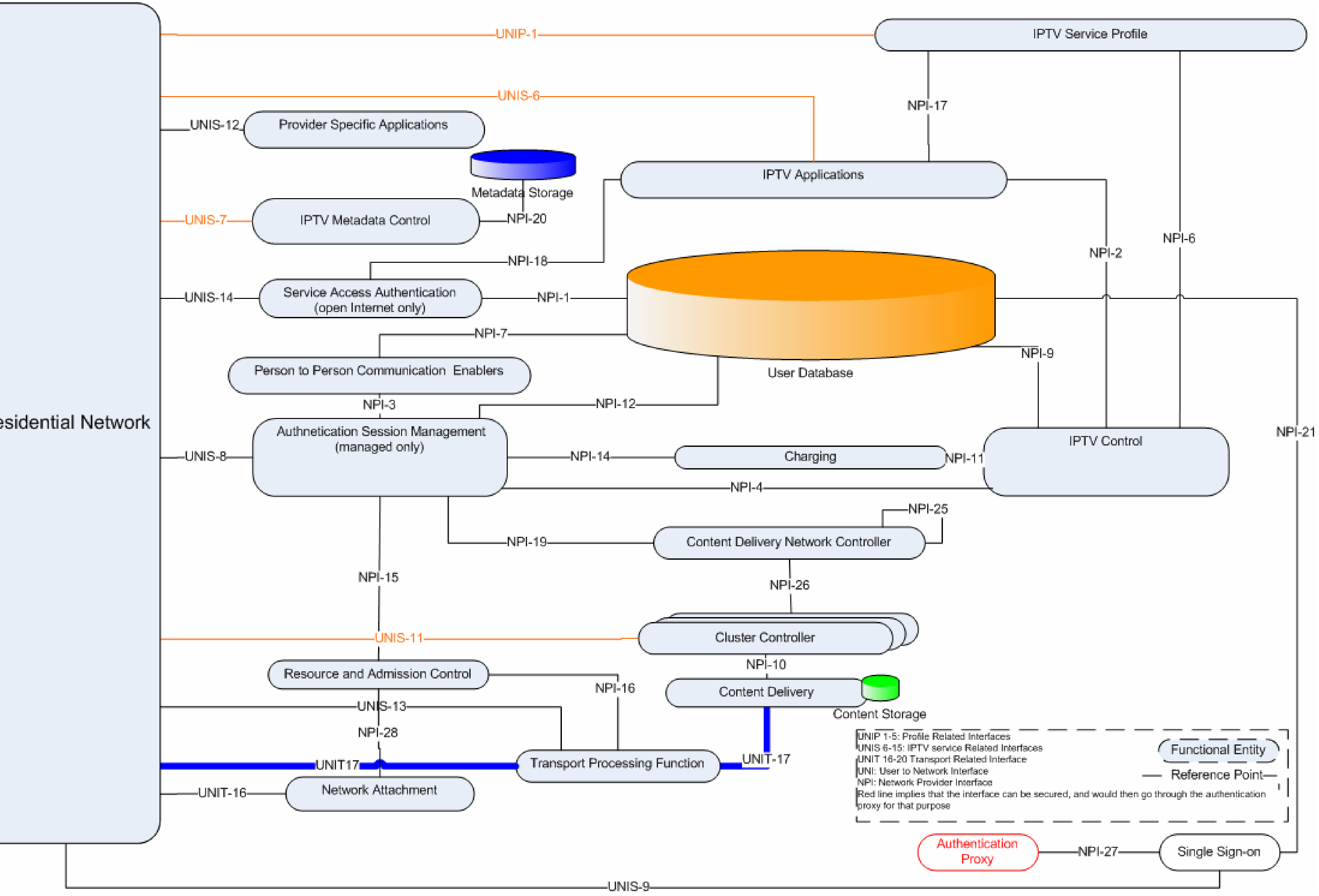

esidential Network
UNIP-1
IPTV Service Profile
UNIS-6
NPI-17
UNIS-12
Provider Specific Applications
Metadata Storage
IPTV Applications
UNIS-7
IPTV Metadata Control
NPI-20
NPI-18
NPI-6
NPI-2
UNIS-14
Service Access Authentication (open Internet only)
NPI-1
NPI-7
Person to Person Communication Enablers
NPI-9
User Database
NPI-3
NPI-12
Authnetication Session Management (managed only)
UNIS-8
NPI-14
Charging
NPI-11
IPTV Control
NPI-21
NPI-4
NPI-25
NPI-19
Content Delivery Network Controller
NPI-15
NPI-26
UNIS-11
Cluster Controller
Resource and Admission Control
NPI-10
NPI-16
Content Delivery
Content Storage
UNIS-13
NPI-28
UNIT17
Transport Processing Function
UNIT-17
UNIT-16
Network Attachment
UNIP 1-5: Profile Related Interfaces
UNIS 6-15: IPTV service Related Interfaces
UNIT 16-20 Transport Related Interface
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
Authentication Proxy
NPI-27
Single Sign-on
UNIS-9

Figure 5.2-1: HLA for managed and unmanaged networks

The following sections describe the functional elements and interfaces depicted in Figure 6.2-1.

5.2.1 Network Provider Functional Entities

The following is a brief description of the functional entities depicted in Figure 6.2-1:

- **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.

- **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 service provider.

- **Service Access Authentication (Unmanaged Only):** This functional entity is responsible for service access protection authentication of users.

- **Authentication and Session Management (Managed Networks 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 IPTV service user profiles as well as other user profile information (for example authentication data) in order to allows it to perform its task.

- **Charging Subsystem**: 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 DRM and CAS). The IPTV service provider's billing mechanisms are out of the scope of this Forum.

- **User Database:** The central database of user 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…

- **IPTV Applications**: These include IPTV related services or applications 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 DA-DLE

- **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 interworks with the session management functionality, which routes incoming requests from the IPTV control to the appropriate destination. This entity has access to the user IPTV service profiles as well as other user profiles information that is needed to deliver personalized user services. The IPTV control generates charging related information.

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

- **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 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:** 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:** 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 entity is responsible for media processing, delivery and distribution, under the control of the Cluster Controller.

- **Resource and Admission Control:** 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.

- **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.

- **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 services such as service discovery, service provisioning and personalized Content Guide (CG). This functional entity enables the user to search, discover and initiate immediate viewing or schedule viewing of future programs and stored content.

- **Authentication Proxy (managed network only):** This functional entity establishes a secure communications channel between a network provider's security domain and the ITF. The Authentication Proxy terminates all signaling 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.

- **Single Sign-on (managed model only):** This functionality allows users to authenticate once with the Service Platform Provider and gain access to services and applications provided by an IPTV Service Provider with whom the SPP has appropriate business and trust relationships.

- **Provider Specific Application:** 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 DA-PLE which can manipulate media streams and the Content Guide.

- **IPTV Service Discovery:** the entry point that provides information necessary for the ITF to select an IPTV service and/or IPTV service provider, in both managed and unmanaged models.

- **DRM:** This functional entity handles service protection and content protection for the DRM client in the home network. 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.).

5.2.2 Mapping between HLA and IPTV Domains (Informative)

The following table provides an informative mapping between the functional entities depicted in the HLA and the IPTV domains as defined in section 5.1.

Table 1: Functional Entity domain assignment

Functional Entity	Notes
Network Attachment	Network Provider
Authentication and Session Management (Managed network only)	Platform Provider
User Database	Platform Provider
IPTV Control	Platform Provider
Person to Person Communication Enablers (Managed network only)	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	Platform Provider
IPTV Service Profile	IPTV Service Provider
Provider Specific Applications	IPTV Service Provider
Metadata Storage	IPTV Service Provider
Service Access Authentication (Unmanaged network only)	Platform Provider
Charging	Platform Provider
Cluster Controller	Network, Platform and IPTV Service Providers
Resource and Admission Control (Managed network only)	Network Provider
Transport Processing Function	Network Provider
Authentication Proxy (Managed network only)	Platform Provider
Single Sign On (Managed network only)	Platform Provider

5.2.3 QoS Framework Architecture Description

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

Resource and Admission Control (RAC) [Ref 13] is the building block responsible for these functions.

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

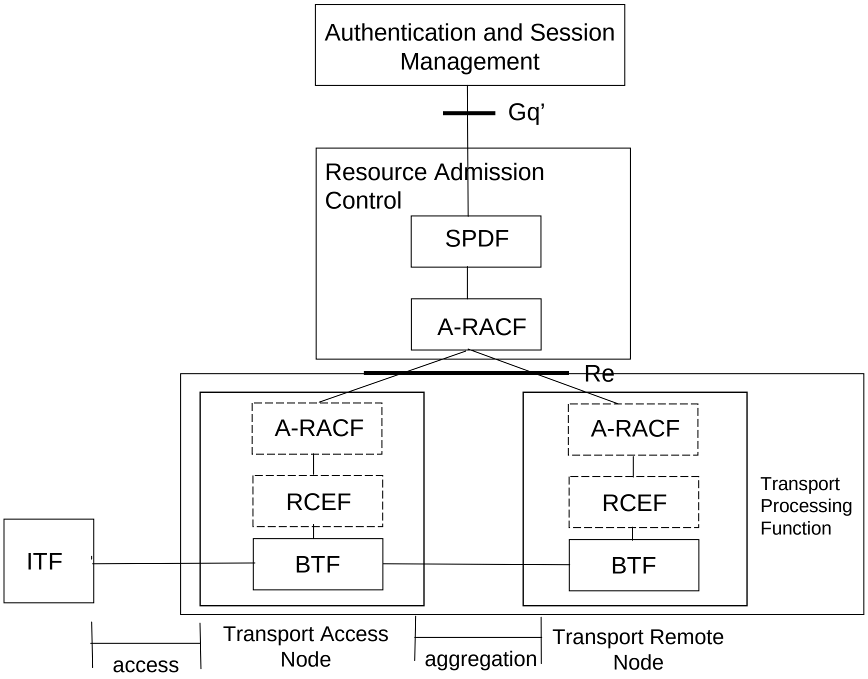
- Authentication and Session Management, receives resource reservation requests and outputs notifications the status of requests
- Transport Processing Functions, enforces policies, receives resource reservation requests and manages the network status
- Network Attachment, receives the subscriber access 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 11] [Ref 12]

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 Annex G for details).

5.2.3.1 RAC functional description and deployment options



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 ASM 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 28] . The RCEF - BTF interface can be considered an internal Transport Processing Functions interface.
- A-RACF – A-RACF: Inter A-RAC interface when multiple A-RACF 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 behavior, with examples of specific deployment scenarios is provided in Annex G.

5.2.4 Reference Points Description

5.2.4.1 UNI Reference Points

Interface Name	*Description*
UNIP-1	Interface for user initiated IPTV service profile management
UNIS-6	User interface to application logic for transfer of user requests and interactive feedback of user responses (provider specific GUI). HTTP is used to interface between the DA-DLE and the IPTV Application Function in both the managed and unmanaged models**.**
UNIS-7	Requests for transport and encoding of content guide metadata. The interface includes the metadata and the protocols used to deliver the metadata, and that shall be standardized based on DVB-IP BCG. [Ref 14]
UNIS-8	Authentication and session management for managed services
UNIS-9	Authentication for Single-Sign on
UNIS-11	User Stream content delivery control interface (Trick mode,) (non aggregated content). This interface is optionally secured. The interface includes content delivery session setup in case of the unmanaged model.
UNIS-12	Interface between the AG and the provider specific application functional entity. Encompasses two functions: • Signalling and download of applications in a generic format. (To be standardised by the Forum) • Interaction of generic applications with the provider network. (Not to be standardised)
UNIS-13	(Managed Network only) User Stream control interface for multicast real time content. The protocol used on this interface is IGMP. [Ref 11]
UNIS-14	Interface used for authorization of service access for the unmanaged network model.

UNIS-15 IPTV Service Discovery (This interface has to be added to the HLA)

UNIT-16 Terminal Attachment functions connected to this interface include: DHCP Server and Relay.

UNIT-17 Content stream including content, both multicast and unicast; content encryption (for protected services) and content encoding. This could be RTP and HTTP.

UNIT-18 RTCP [Ref 15] based interface . (This interfaces have to be added to the HLA)

UNI-RMS Remote Management of end user devices (based on DSL Forum TR69) [Ref 1] (This interface has to be added to the HLA)

UNIS-DRM Rights management for protected content – including key management and rights expression. (This interface has to be added to the HLA)

5.2.4.2 Network Reference Points Description

Interface Name ***Description***

NPI-1 Interface between the service access authentication and the user database.

NPI-2 An optional reference point allowing interaction between IPTV applications and the IPTV Control Point. This is not subject to standardization.

NPI-3 The service interface between authentication session management and person to person communication (ISC interface) [Ref 2]

NPI-4 Interface for routing of IPTV service related messages to the IPTV Control Point. This is the ISC reference point defined by 3GPP. [Ref 2]

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. This interface is 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 2]

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 2]

NPI-10 An optional reference point for the allocation/de-allocation and control of content for a specific unicast session. This reference point is not subject to standardization [UNDER REVIEW]

NPI-11 An interface for sending events and charging information. This is the Rf reference point defined by 3GPP.[Ref 2]

NPI-12 This reference point allows the authentication and session management functionality to retrieve subscriber IMS data from the HSS as a part of the user’s IMS registration. This is the Cx interface defined by 3GPP.[Ref 2]

NPI-14 Same as NPI-11

NPI-15 This interface controls the Resources and Admission Control. It is the Gq interface defined by 3GPP. [Ref 2]

NPI-16 Interface between the Transport and Multicast Delivery and Resource and Admission Control. It is the Re interface (Diameter based) [Ref 2]

NPI-17 Interface between the IPTV Applications and the IPTV service profile. Only needed for the unmanaged network model.

NPI-18	Interface between the Service Access and Authentication function and the IPTV applications. Only in the unmanaged model
NPI-19	This interface 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. This is not subject to standardization
NPI-21	This interface allows the Single-sign on function to validate user credentials
NPI-25	This interface allows proxying unicast control messages to locate the appropriate content delivery control function.
NPI-26	The interface allows the content delivery network controller to delegate the handling of a unicast session to a specific cluster.
NPI-27	The interface between the Authentication Proxy and the Single Sign-On node allows the proxy to retrieve a user key for authentication purposes.
NPI-28	This interface is used to push the user access capabilities to the network attachment and RAC. This the e4 interface. [Ref 2]

5.3 Residential Network High-Level Architectural Overview

The architecture of the consumer domain (referred to hereafter as the residential network architecture) is composed of 4 functional entities, with well defined interfaces between them, and where each functional entity includes a number of functions.

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 6.3.-1 below.

There are two main interface groups between the residential network and the network provider domain: the HNI-INI and the HNI-AMNI. The mapping between these key functional groupings and UNI reference points is depicted in the figure 6.3-1.

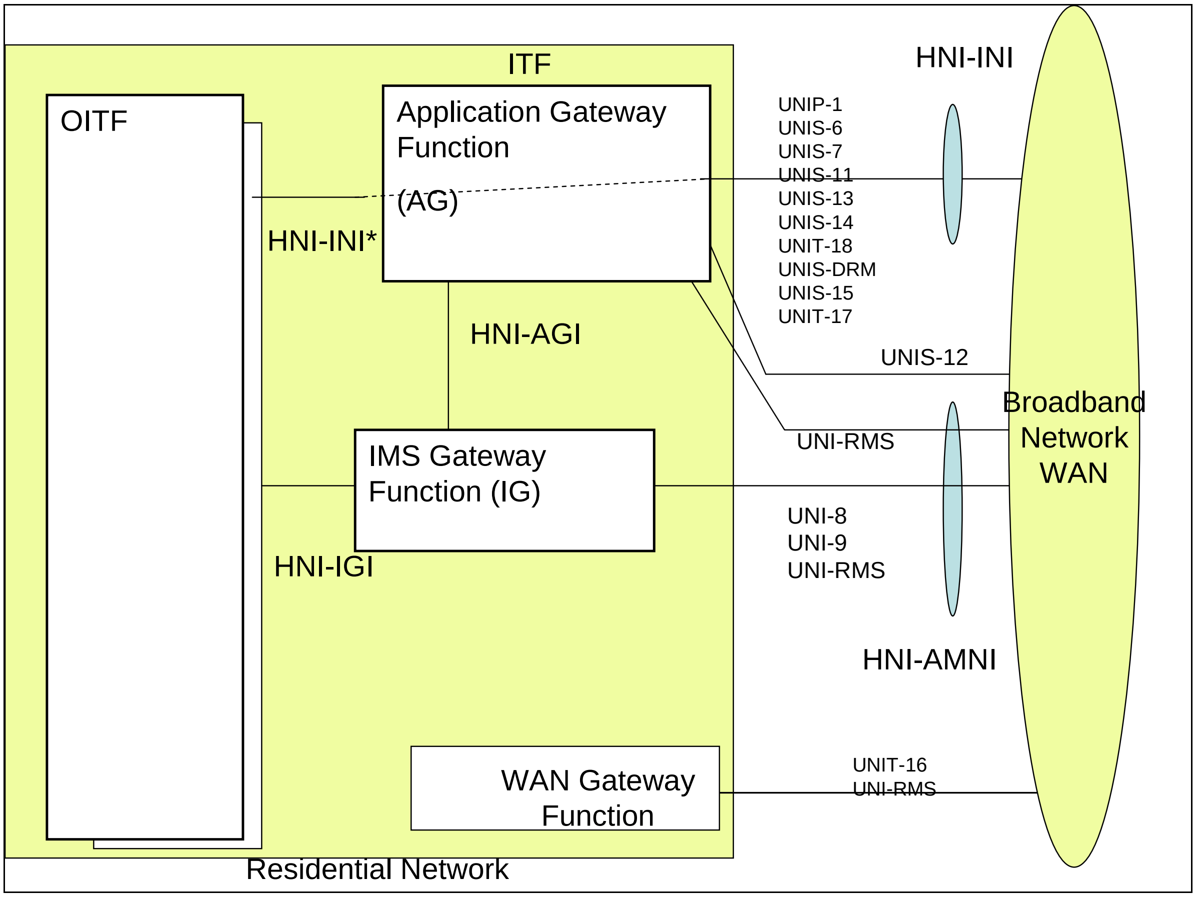


Figure 6.3-1: Residential Network Architectures

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 implementation of the HN-INI and HN-AMI 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.

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 3].

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. 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 are those that insert personalized ads in media stream, or full blended person-to-person communication services. 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 goal is for the HN-INI* to be the same as the HN-INI interface.

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

- Manipulate media streams
- Filter CG data and insert its own CG data
- Support proprietary applications through a Remote User Interface.
- Support advanced blended communication services.

The AG is able to make use of the services of the IG via the HNI-AGI interface.

4). WAN Gateway Functional Entity

The WAN Gateway function supports the physical connection between the home LAN network 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 the detailed functional description of the residential network, this specification uses a stepwise build up of the HN functional entities comprising of the following steps:-

- OITF and WAN Gateway (WG)
- OITF, WG and IG
- OITF, WG, IG and AG

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 and WAN Gateway functional entities may be deployed as separate physical devices in the residential network or in combinations as described in Section 5.3.3.

5.3.1.1 OITF

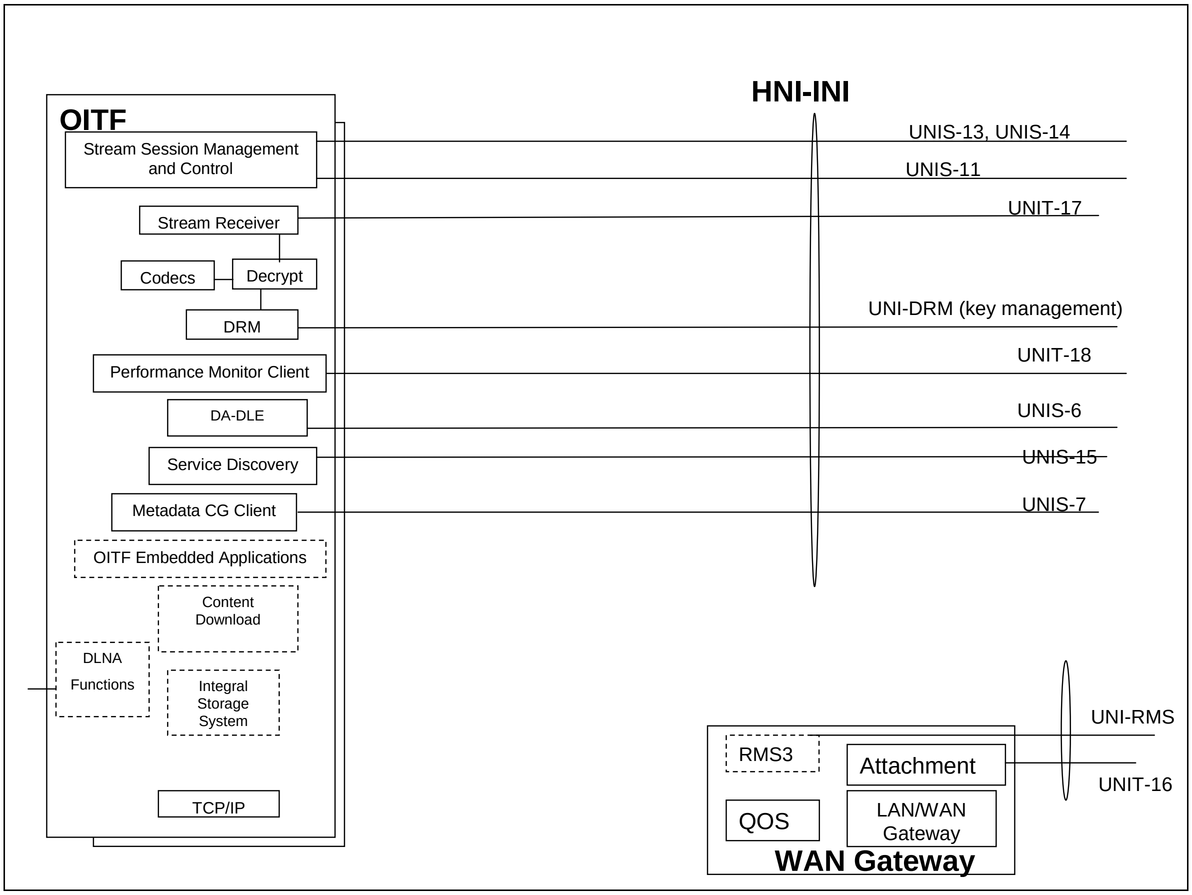


Figure 6.3-2: OITF functions and interfaces exposed

The **OITF** includes the following functions:

Stream Session Management and Control: Initiates and closes 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.

DRM: Client side key management for service protection and content protection. Enforces content usage rules in the client. It applies to both the managed and the unmanaged models.

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

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

Downloaded Application - Declarative Language Environment (DA-DLE): A declarative language based environment (browser) based on CEA 2014 [Ref 4]for presentation of user interface and including scripting support for interaction with network server-side applications and access to the APIs to the other OITF functional entities.

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

The downloaded applications that are run in the DA-DLE 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 interaction with this client is vendor dependent. This function may also make the metadata available to Residential Network devices via the DLNA DMS Gateway function. It applies to both the managed and the unmanaged models.

IPTV Service Discovery: Functional entity for discovering IPTV Service Providers. Applies to both the unmanaged and the managed models. Note that different aspects of DVB SD&S [Ref 5]may apply to the different models.

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

DLNA functions: Implements DLNA DMS [Ref 3] functions to expose and distribute content in a DLNA compliant manner through the residential network. The DLNA gateway may also offer a DLNA DMP [Ref 4] function to locate content available from other DMS in the residential network and receive a stream it for rendering by the OITF streaming client. This block 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 HN-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 (exact information to be provided is to be specified by the OIPTV Specification). It applies to both the managed and the unmanaged models.

The **WAN** Gateway Functional Entity contains the following functions:

LAN/WAN gateway: Supports the physical termination of the access providers 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 access provider network.

RMS: 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.)

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 7] 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.

5.3.1.2 OITF and IG

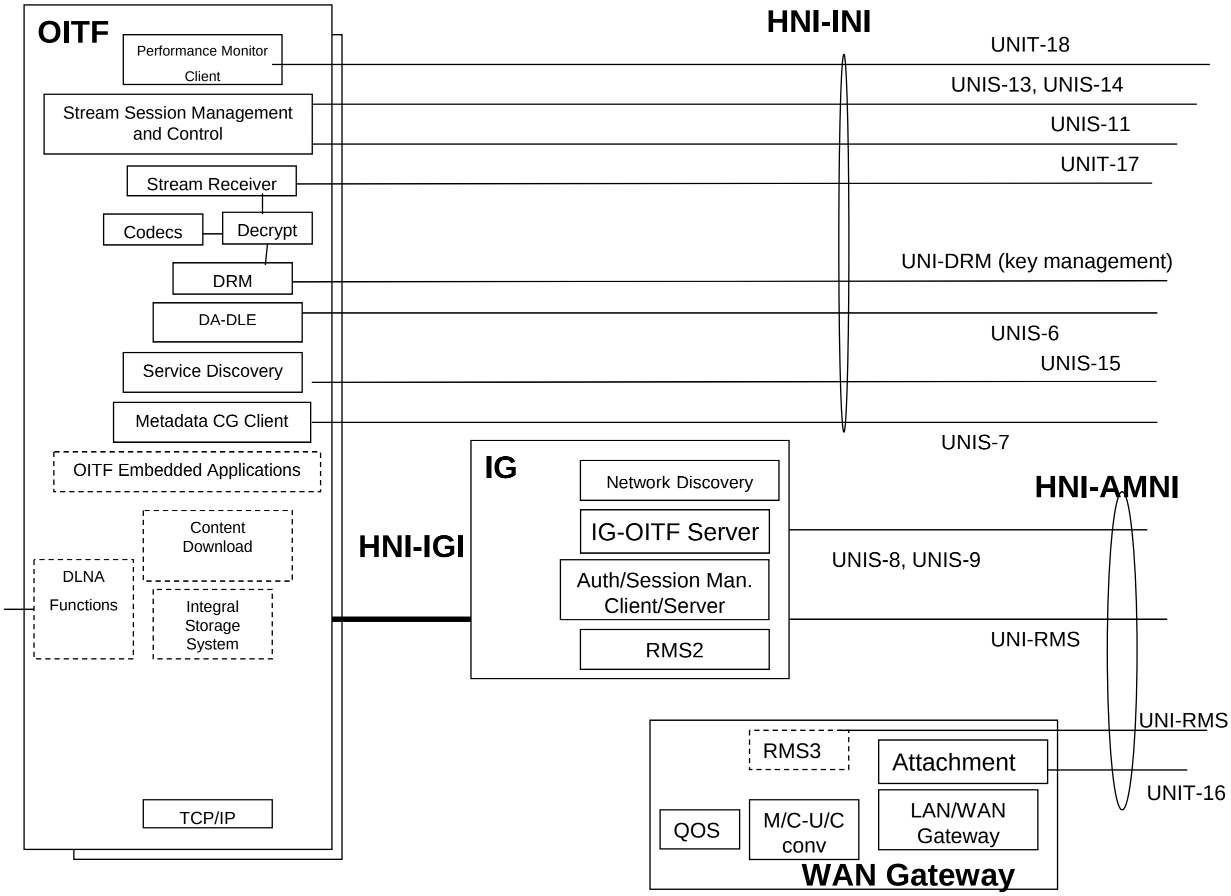


Figure 6.3-3: OITF and IG

The IG depicted in Figure 6.3-3 includes the following additional functions:

IG – IMS Gateway

Authentication and 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 communications services).

The authentication and session management functional entity 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 the HTTP based protocol. 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 DA-DLE function on the OITF.

RMS 2: Client application for remote management functions in a managed environment. It provides a standard interface for provisioning and assurance tasks on managed OIF devices. It includes functions for configuration management, firmware upgrade, troubleshooting/diagnostics, performance management and monitoring of streaming 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 and AG

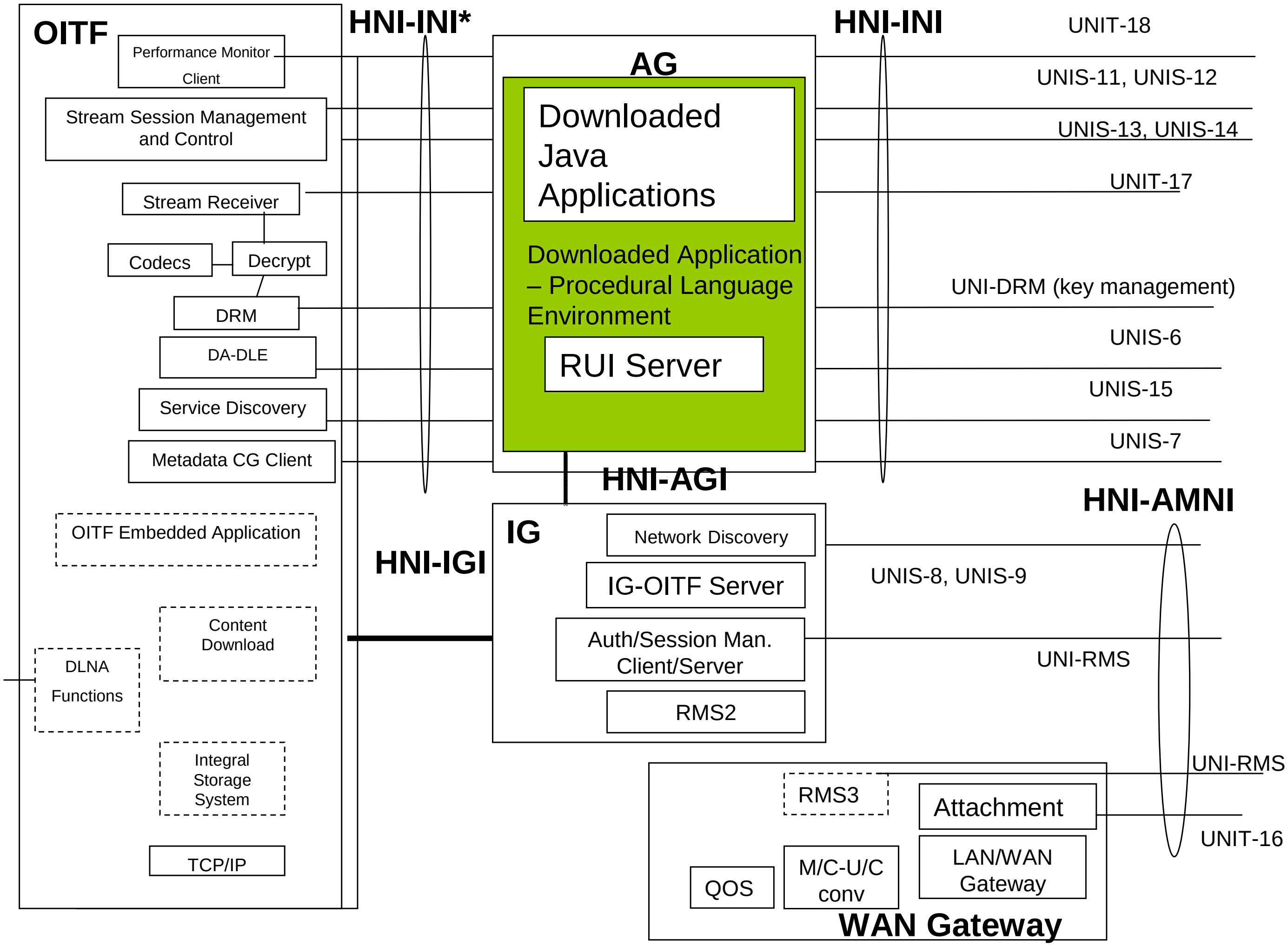


Figure.6.3-4: All HN Functional entities

A residential network with the addition of an Application Gateway to the OITF/IG/WG configuration is depicted in Figure 6.3-4.. This represents a residential network with all the functions defined by the HN functional entities. The following additional functions are defined in the Application Gateway.

Application Gateway

Downloaded Application – Procedural Language Environment (DA-PLE): A local procedural language execution environment based on Java CDC for Service Provider specific down loaded applications. If required, these applications can present a UI via the CEA-2014 [Ref 3] based Remote UI function on the OITF’s DA-DLE.

The definition of the full capabilities of the DAPLE is within the scope of the OIPTVF. 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 DA-PLE 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, DRM) 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 DAPLE via defined APIs.
- **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 DADLE
      - Passing all or some subset of the metadata to the "Metadata CG client" on the OITF, depending on the policy of the operator.

  When present, this application terminates the UNIS-7 interface. Otherwise, the CG application client in the OITF directly handles the UNIS-7 interface.

  Furthermore, in the case of a managed network, the service provider has the option, subject to operator policy, of passing all or some of the metadata to the "Metadata CG client "on the OITF, or making a complete presentation to the GUI engine via the DA-DLE, bypassing completely the "Metadata CG client" in this case.

  Note that this option is only applicable for deployment purposes. From a conformance point of view both options must be supported.

- **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 telephony. The IG-AG 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 DA-PLE to serve declarative language applications running on the DA-DLE in the OITF.

5.3.2 Multicast Handling in modem gateway router [Under Review]

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.

5.3.2.1 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 6-6.

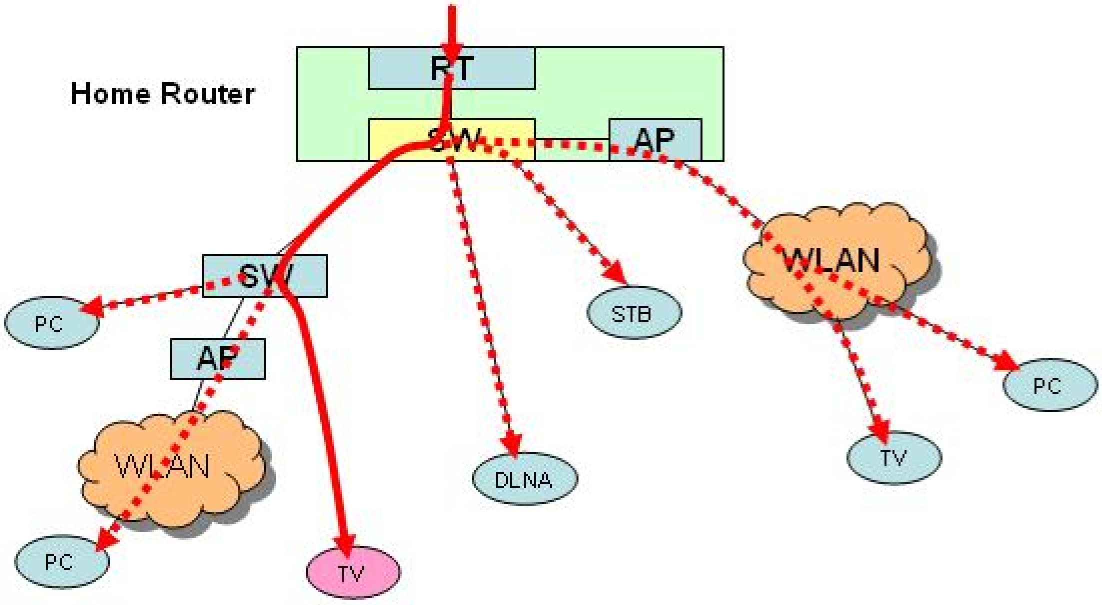


Figure 6.3-4: Example of flooding issue

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 8]

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 9] and managing the membership of multicast listeners.

In this release of the architecture, support of IGMP snooping and IGMP proxy [Ref 10] is mandatory to avoid flooding of unnecessary segments.

5.3.2.2 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.

5.3.3 Deployment Options [Under Review]

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

Table [XXX] shows the possible deployment options and how they are used.

Functions deployed in the residential network				**Services available**
WAN-G	**OITF**	**IG**	**AG**	
X	X			Unmanaged services only are available.

				DA-DLE applications can be deployed.
X	X	X		Managed network and Unmanaged services are available. DA-DLE applications can be deployed.
X	X	X	X	Managed network and Unmanaged services are available. DA-DLE and DA-PLE applications can be deployed.
X	X		X	[This deployment option is not supported by this version of the specification] Unmanaged services are available. DA-DLE and DA-PLE applications can be deployed.

5.3.3.1 Combined Devices

Each of OITF, IG, AG and WAN Gateway functional entities may be deployed as separate devices within the residential network. It is also possible to combine two or more functional entities in a single physical device in any combination.

When a physical device includes more than one functional entity, interfaces wholly between the combined functional entities are considered internal to the device and need not meet the requirements set out by the Forum's specifications – in any case, these interfaces are not externally verifiable. The device shall meet the requirements of this specification for all interfaces to functional entities that are not included in the physical device.

5.3.4 Residential Network Reference Points

- **HNI-INI**: This interface 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 as described in section 6.3.1.2. The HNI-INI consists of the following UNI reference points.
    - **UNIP-1 (User initiated profile management)**
    - **UNIS-13 (Stream Session Management and Control)**
    - **UNIS-11 (Stream Session Management and Control)**
    - **UNIS-DRM (to "DRM")**
    - **UNIS-6 (to "DL-DLE")**
    - **UNIS-7 (to "Metadata based Content Guide client")**
    - **UNIT-17 (Stream receiver)**
    - **Etc.**
- **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. The HNI-INI* includes the device discovery mechanisms.
- **HNI-IGI**: This interface is between the OITF and IG and provides IG functions for the adaptation to IPTV services on managed networks. The HNI-IG includes the device discovery mechanisms.
- **HNI-AGI:** This interface is between the IG and AG and provides IG functions for the adaptation to IPTV services in managed networks. The HNI-IG includes the 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.

6. High Level Signalling Flows (Informative)

6.1 Network Attachment

To be provided

6.2 IPTV Service Discovery and Selection [Under Review]

6.2.1 Bootstrap procedure for IPTV Service Discovery

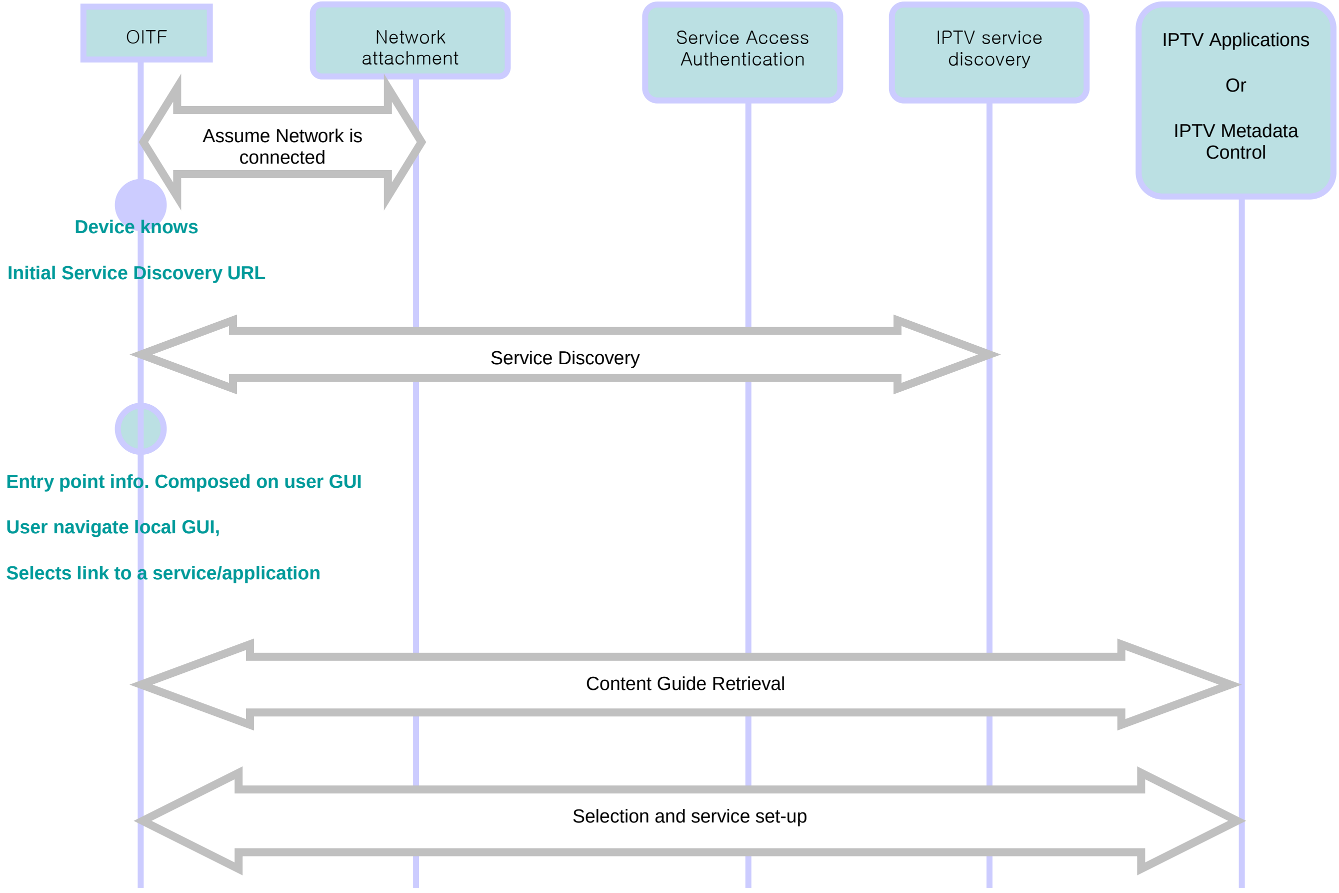
To be provided.

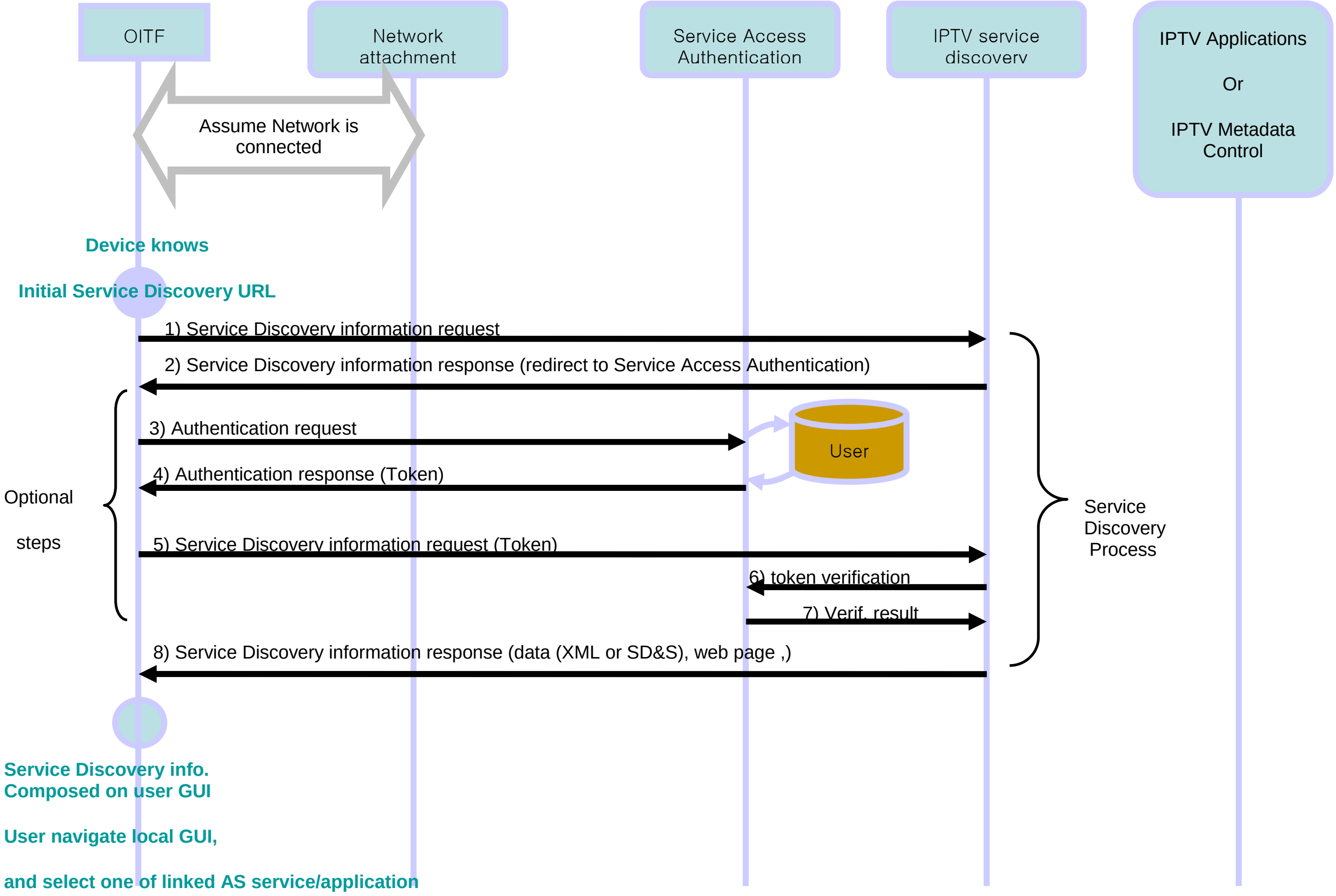
6.2.2 Unmanaged model service provider discovery and selection

6.2.2.1 Service provider discovery

6.2.2.2 Service provider selection

The following sequences show a high level call flow for IPTV Service Provider discovery followed by content guide retrieval and service selection. Each call flow can include an optional authentication step.


OITF
Network attachment
Service Access Authentication
IPTV service discovery
IPTV Applications
Or
IPTV Metadata Control
Assume Network is connected
Device knows
Initial Service Discovery URL
Service Discovery
Entry point info. Composed on user GUI
User navigate local GUI,
Selects link to a service/application
Content Guide Retrieval
Selection and service set-up


OITF
Network attachment
Service Access Authentication
IPTV service discovery
IPTV Applications
Or
IPTV Metadata Control
Assume Network is connected
Device knows
Initial Service Discovery URL
1) Service Discovery information request
2) Service Discovery information response (redirect to Service Access Authentication)
3) Authentication request
User
4) Authentication response (Token)
Optional
steps
5) Service Discovery information request (Token)
6) token verification
7) Verif. result
Service Discovery Process
8) Service Discovery information response (data (XML or SD&S), web page ,)
Service Discovery info. Composed on user GUI
User navigate local GUI,
and select one of linked AS service/application

The following steps describe the above call flow:

1) The ITF sends the IPTV Service Discovery information request to the IPTV Service Discovery functions, whose URL is pre-configured on entered manually/automatically

2) The IPTV Service Discovery functions sends back a link containing the IPTV service discovery URL, asking the OITF to authenticate itself towards it (HTTP redirect);

3) The Authentication request , with the credentials (user and/or terminal credentials), is sent to the Service Access Authentication

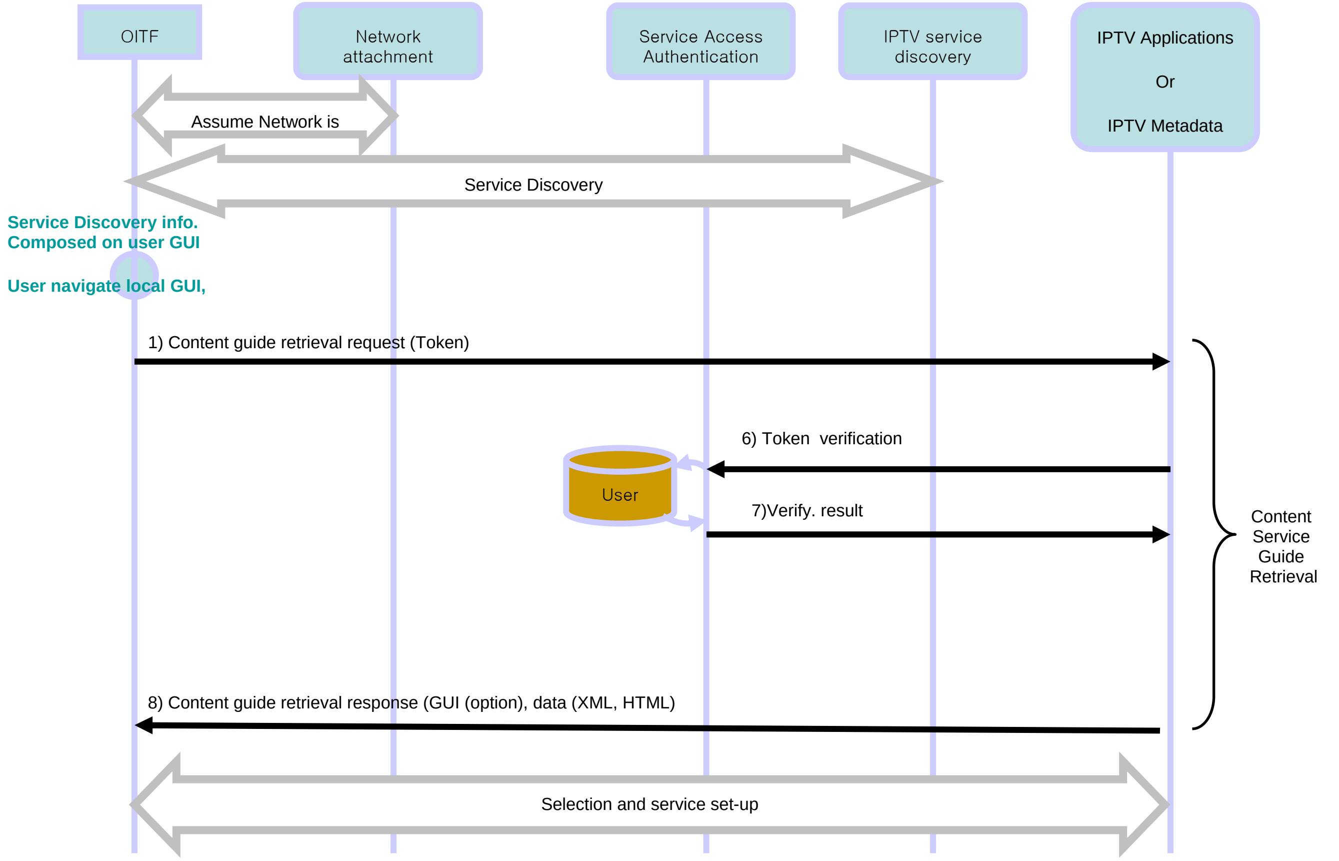
4) The Service Access Authentication authenticated the credentials, after querying the user database, and sends back the authentication token to be used by OITF; (more steps could occur between 3 and for depending on the authentication mechanism)

5) The OITF resends the IPTV Service Discovery information request to the IPTV Service Discovery function, including the authentication token in the request

6) The IPTV service discovery checks towards the Service Access Authentication functions the token

7) The authentication result is sent back to the IPTV Service Discovery

8) The IPTV Service Discovery functions sends back to OITF the Service Discovery information which could be a xml data or a web page [details to be determined by the solutions WG]


OITF
Network attachment
Service Access Authentication
IPTV service discovery
IPTV Applications Or IPTV Metadata
Assume Network is
Service Discovery
Service Discovery info. Composed on user GUI
User navigate local GUI,
1) Content guide retrieval request (Token)
6) Token verification
User
7)Verify. result
Content Service Guide Retrieval
8) Content guide retrieval response (GUI (option), data (XML, HTML)
Selection and service set-up

We assume that the OITF has already discovered the Service through an IPTV Service Discovery procedure and already has a token.

1) The ITF sends the content guide retrieval request to the IPTV Applications or IPTV Metadata Control

6) The IPTV Applications or IPTV Metadata Control checks towards the Service Access Authentication functions the token

7) The authentication result is sent back to the IPTV Applications or IPTV Metadata Control

8) The IPTV Applications or IPTV Metadata Control sends back to OITF the IPTV Content Guide information

6.2.3 Managed model service provider discovery

To be provided.

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 16] 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.

6.3.1 Unmanaged Networks

For unmanaged networks, the solution should use HTTP Digest Authentication [RFC 2617] [Ref 17] 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. The following figure depicts the call flow for HTTP Digest Authentication between the relevant functional entities.

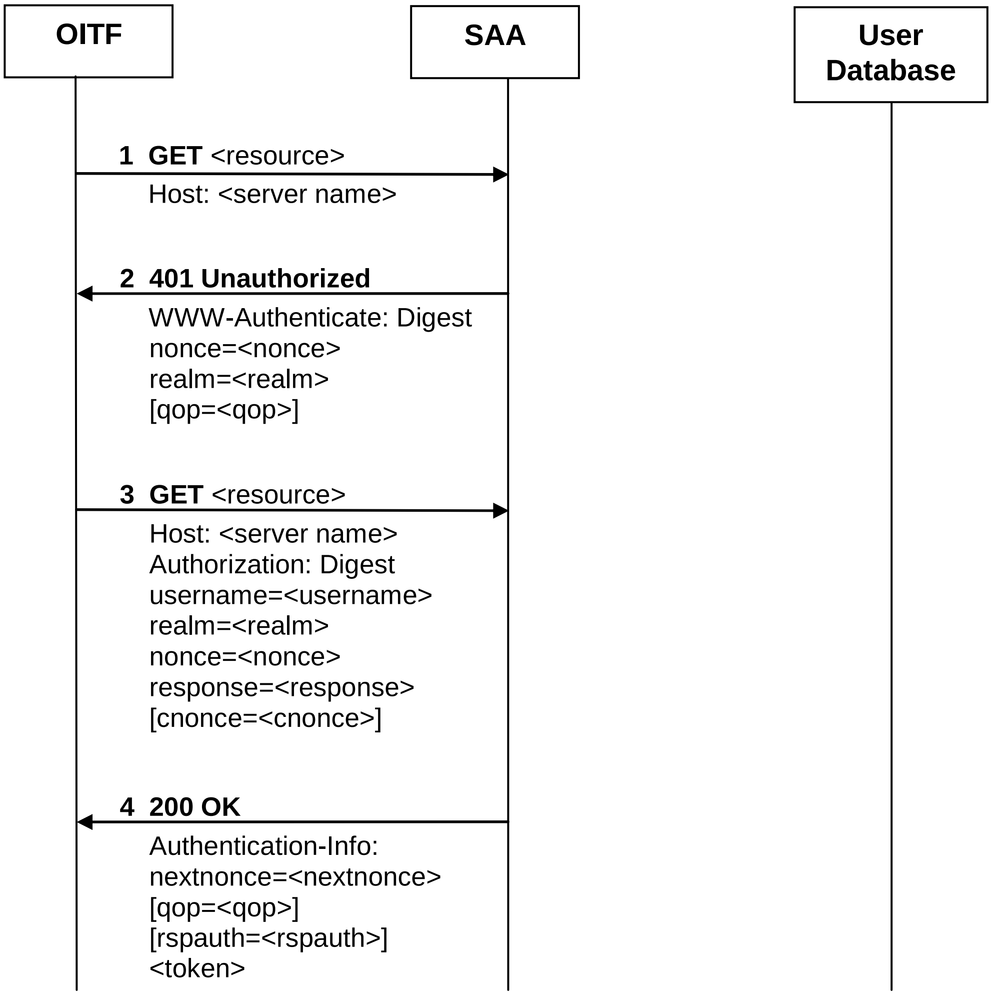


Figure 1: Identification and Authentication using HTTP Digest in the case of unmanaged networks

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 IPTV Client can be authenticated by the HTTP Server 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 a token that the OITF can later on send to the IPTV Service Discovery function so that this function is able to verify that the OITF has been successfully authenticated by the SAA function. In case the HTTP Server 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 HTTP Server in step 3. This rspauthn value enables the IPTV Client to authenticate the HTTP Server.

6.3.2 Managed Networks

In the managed network case, user identification and authentication is based on either 3GPP IMS Authentication and Key Agreement (AKA) as defined by TS 33.203 [Ref 18], or on TISPAN HTTP Digest [Ref 19] .

Registration 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 Home of the ISIM’s or USIM’s residential network (operator network). The following figure shows the high-level message flows for user identification and authentication based on the IMS AKA procedure:

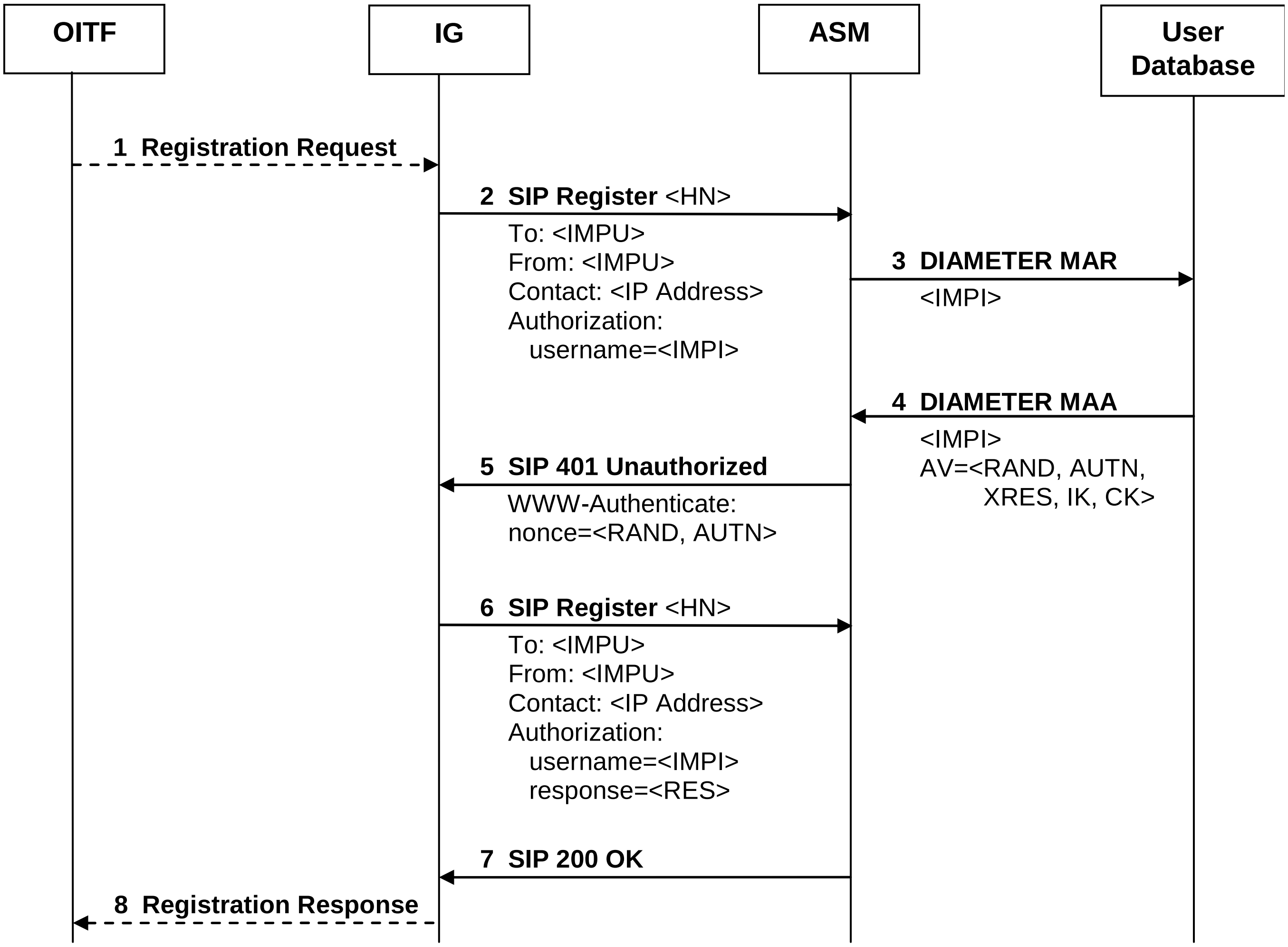


Figure 2 : Identification and Authentication using IMS AKA in the managed case

The following is a description of the message flows shown above:

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 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 TISPAN HTTP Digest

TISPAN HTTP Digest will follow the specification, which is a work in progress

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:

1. CoD, Content on Demand: End users can order videos through a CoD catalogue and have them streamed directly to the ITF
2. nPVR, Network based Personal Video Recorder: Allows recording of programs on the network side, and delivered as a unicast stream when played back .
3. 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) result in a unicast nPVR session.

6.4.1 Unicast Session Set up (managed model)

Figure 6.4-1 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

We will describe each of those call flows in separate sub-paragraphs

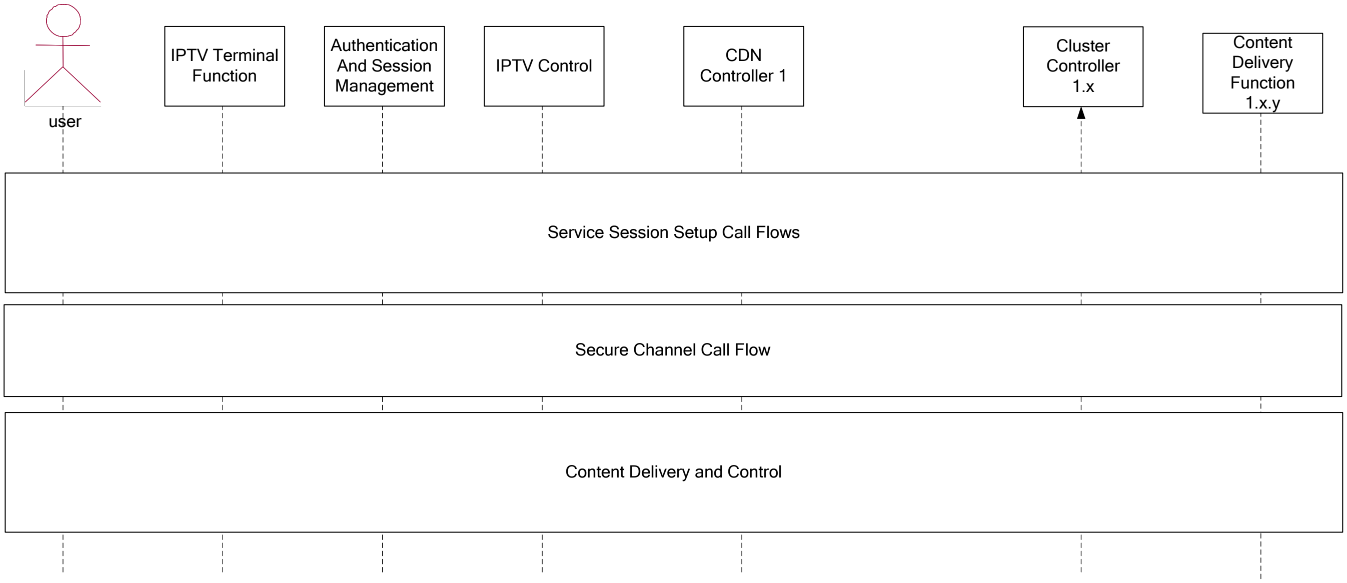

user
IPTV Terminal Function
Authentication And Session Management
IPTV Control
CDN Controller 1
Cluster Controller 1.x
Content Delivery Function 1.x.y
Service Session Setup Call Flows
Secure Channel Call Flow
Content Delivery and Control

Figure 6.4-1: Overall Description of the call flows

6.4.1.1 Service Session Setup Description

The service session establishment in the managed model involves the ITF, the IPTV Control, the CDN the "Authentication and Session management" and "Resource and Admission Control" functional entities. See Figure 6.5-2

- Signal 1 ("Request the video"): the sequence is triggered by an action from the user. The user requests something from the CoD catalogue or selecting some content stored in an nPVR, which results in a unicast session.
- The IPTV Terminal Function gets the information about the content that is displayed to the user from the IPTV Metadata Control or any other source. The information includes whatever is necessary to make an SDP offer. The SDP offer must include the IP addresses and ports of the OITF, which is the destination address of the stream.
- Signal 2 ("Service Session Setup Request"): the ITF sends a session setup request to the Authentication and Session Management functional entity. The request includes the selected content id and the corresponding SDP offer.
- Exchange A: Resource Reservation Phase. The "Authentication and Session Management" uses the services of the "Resource and Admission Control" FE to perform resource reservation.
- Signal 3 ("Service Session Setup Request"): The request is forwarded to the IPTV Control functional entity where it is authorized (signal 4: Validate the Request) based on the user profile stored there or fetched if needed. The requested video file is identified (signal 5 “Video file selection”).
- Signals 6 and 7 ("Service Session Setup Request"): the IPTV Control functional entity forwards the request, via the Authentication and Session Management, to the appropriate Content Delivery Network Controller functional entity

that can handle that request. The selection of the appropriate CDN controller is done by either the IPTV Control FE or indirectly as described in C.2.1.

- Signal 8 ("CC choice"): The target Content Delivery Network Controller locates the appropriate Cluster by choosing the appropriate "Cluster controller".
- Signal 9 ("Delivery Session Setup Request"): the Content Delivery Network Controller forwards the session setup request to the chosen "Cluster Controller"
- Signal 10 ("CDF choice"): the Cluster Controller analyses the session setup 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 for more information about CDNC/CC/CDF selection.
- Message exchange 11: The Cluster Controller fetches the content delivery information (e.g. RTSP Describe) from the Content Delivery Function and sets up the content delivery session for the requested content (e.g. using RTSP Setup).
- Signals 12-15: the Content Delivery Session identification is relayed back through the Authentication and Session Management entity to the ITF.
- Exchange A (between Signals 14 and 15): Resource Commit Phase. The "Authentication and Session Management" instructs the "Resource and Admission Control" to commit the reserved resources.

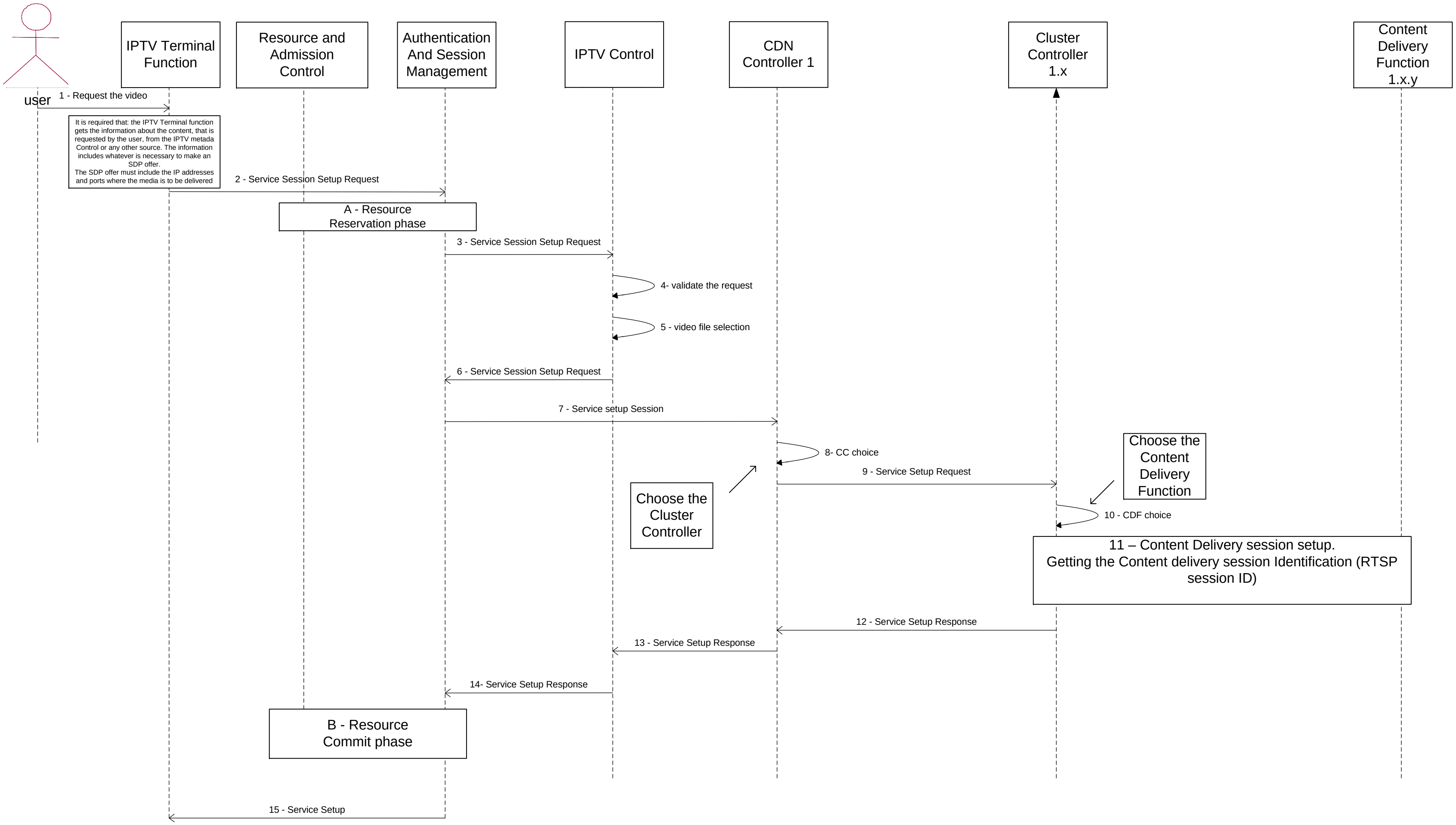

user
IPTV Terminal Function
Resource and Admission Control
Authentication And Session Management
IPTV Control
CDN Controller 1
Cluster Controller 1.x
Content Delivery Function 1.x.y
1 - Request the video
It is required that: the IPTV Terminal function gets the information about the content, that is requested by the user, from the IPTV metada Control or any other source. The information includes whatever is necessary to make an SDP offer.
The SDP offer must include the IP addresses and ports where the media is to be delivered
2 - Service Session Setup Request
A - Resource Reservation phase
3 - Service Session Setup Request
4- validate the request
5 - video file selection
6 - Service Session Setup Request
7 - Service setup Session
8- CC choice
Choose the Cluster Controller
9 - Service Setup Request
Choose the Content Delivery Function
10 - CDF choice
11 – Content Delivery session setup.
Getting the Content delivery session Identification (RTSP session ID)
12 - Service Setup Response
13 - Service Setup Response
14- Service Setup Response
B - Resource Commit phase
15 - Service Setup

Figure 6.5-2: Service Session Setup Call Flow

6.4.1.2 Securing Content Delivery Session Signalling (optional)

As shown in Figure 7.5-3, a secure channel is established between the ITF and the Cluster Controller prior to any exchange of signalling messages. In particular, this allows the Cluster Controller and the ITF 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.

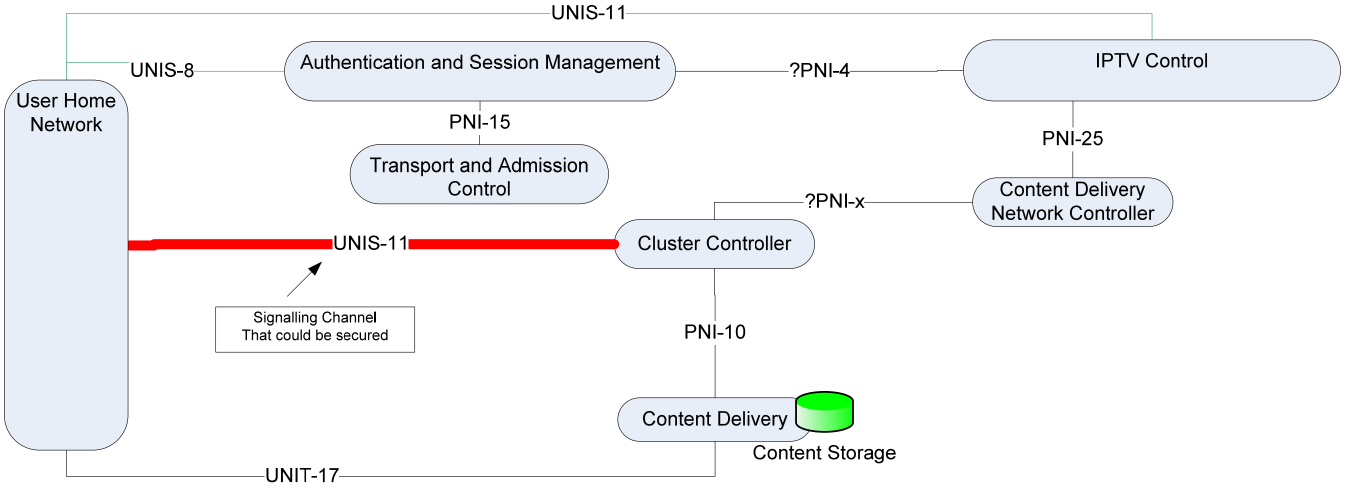

UNIS-11
UNIS-8
Authentication and Session Management
?PNI-4
IPTV Control
User Home Network
PNI-15
Transport and Admission Control
PNI-25
Content Delivery Network Controller
?PNI-x
UNIS-11
Cluster Controller
Signalling Channel That could be secured
PNI-10
Content Delivery
Content Storage
UNIT-17

Figure 7.5-3: Overall architecture of the functions needed for unicast including the secure tunnel

Figure 7.5-4 depicts the actual call flow for setting up such a secure tunnel..

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

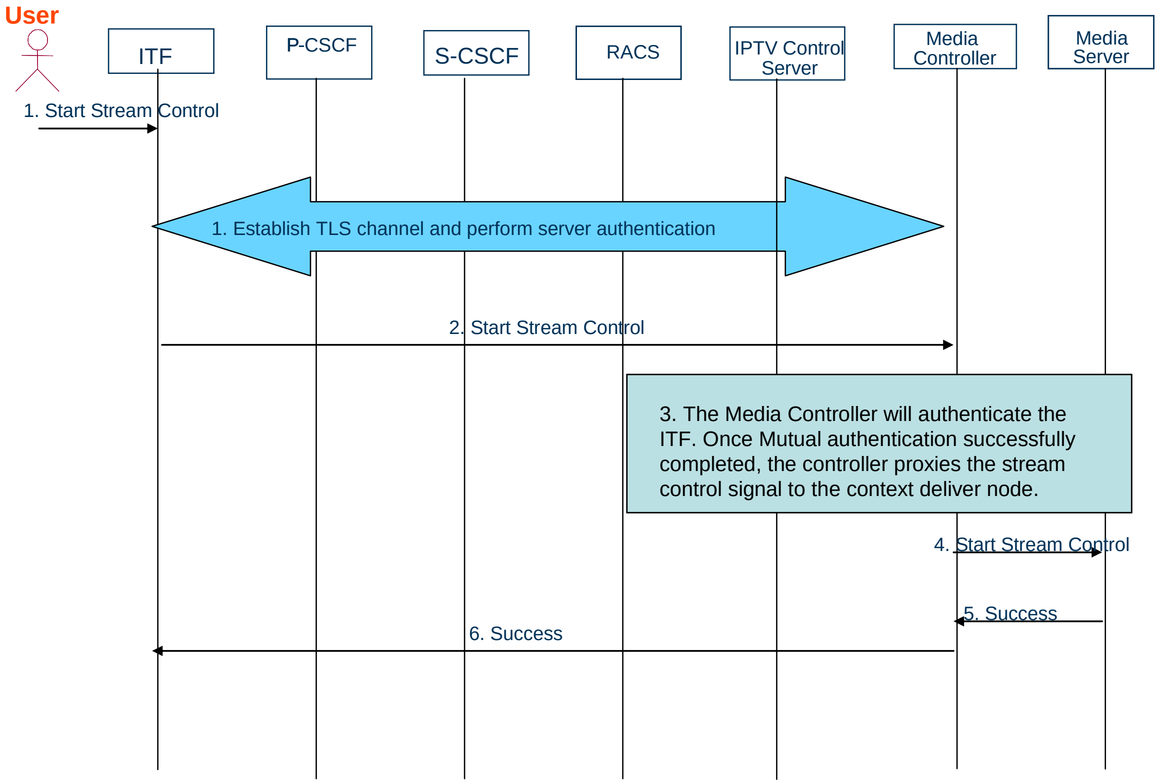

User
ITF
P-CSCF
S-CSCF
RACS
IPTV Control Server
Media Controller
Media Server
1. Start Stream Control
1. Establish TLS channel and perform server authentication
2. Start Stream Control
3. The Media Controller will authenticate the ITF. Once Mutual authentication successfully completed, the controller proxies the stream control signal to the context deliver node.
4. Start Stream Control
5. Success
6. Success

Figure 6.5-4: Securing the Content Delivery Signalling

6.4.1.3 Content Delivery

After the service and content delivery sessions are setup, as explained in section 6.4.1.1, the ITF uses the content delivery session ID to stream the content from the CDF. A logical binding exists between the service setup session and the content delivery session. The binding is done by the CC.

The steps in this call flow are as follows.

5- 6- The request to start streaming is forwarded by the Cluster Controller to the Content Delivery Function.

7- The Content Delivery Function starts streaming the media directly to the ITF.

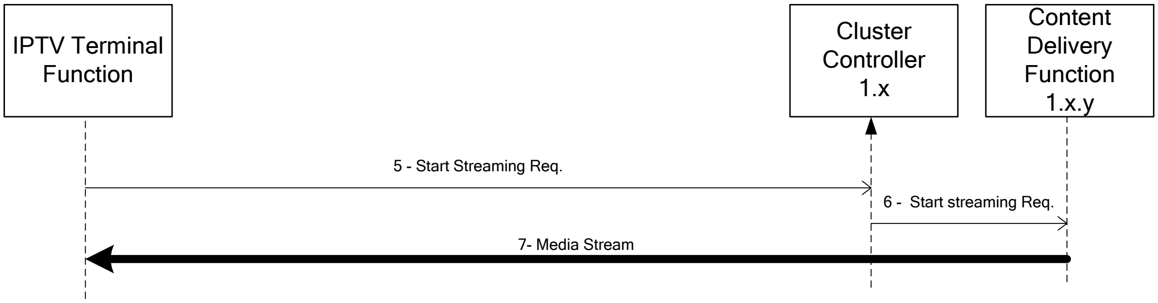


Figure 6.5-5: Content Delivery Session Establishment

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 ITF or from the network side. The subsequent call flows shows both cases for exemplary purposes.

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

6.4.2.1 Client initiated Session Modification Call Flow

Figure 6..5-6 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 prior to any modification, a Service Session and its associated Content Delivery Session(s) have been established.

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

The sequence is triggered by an action from the user. The user requests a new stream to be added to an existing unicast session.

- In step 1, the ITF sends a session modification request to the Authentication and Session Management functional entity. The request includes the selected content.
- Steps 2-3 are optional and are only applicable for managed networks. In those steps, the Session Management functionality verifies with the Network Resource Controller/Admission Control functionality the availability of necessary network resources to handle the requested content..
- In step 4, the request is forwarded to the IPTV Control, where the request is authorized based on the user profile stored there or fetched if needed.
- In step 5, the IPTV Control FE forwards the request to the Session Management to be routed to the appropriate Cluster Controller function that should be contacted to handle that request. (Please check Appendix C for more information about CDNC/CC/CDF selection.)
- In step 6, the Authentication and Session Management FE forwards the request to the target CDNC/CC function.

- In step 7, the target CC FE locates the appropriate CD FE for the requested content and sets up a streaming session with it for the purpose of exchanging addressing information. Other information may also be exchanged within that request.
- In step 8, the CD FE responds with the necessary addressing information for its end, as well as the network resources needs for the requested content. Other information may also be exchanged within that response

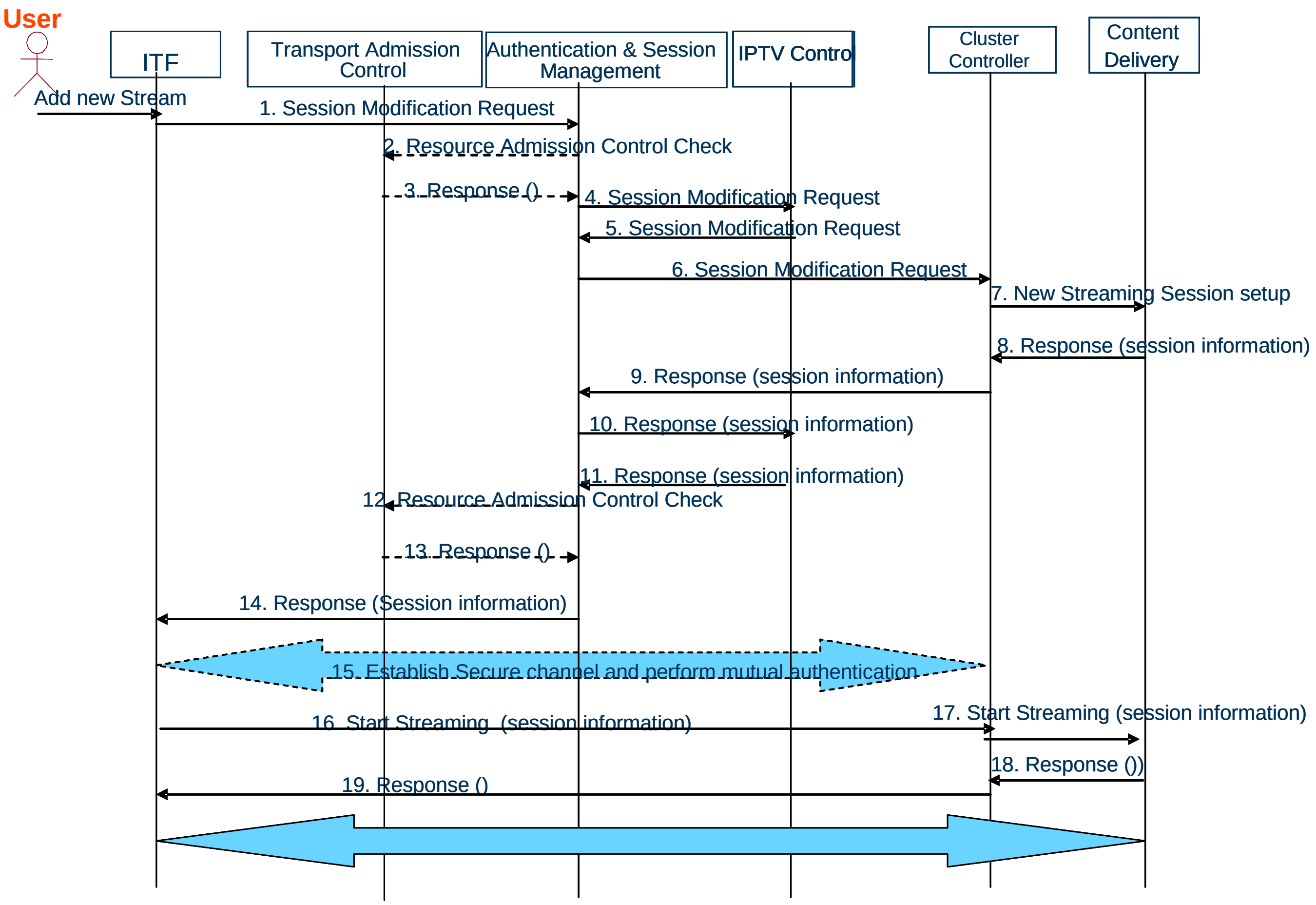

User
ITF
Transport Admission Control
Authentication & Session Management
IPTV Contro
Cluster Controller
Content Delivery
Add new Stream
1. Session Modification Request
2. Resource Admission Control Check
3. Response ()
4. Session Modification Request
5. Session Modification Request
6. Session Modification Request
7. New Streaming Session setup
8. Response (session information)
9. Response (session information)
10. Response (session information)
11. Response (session information)
12. Resource Admission Control Check
13. Response ()
14. Response (Session information)
15. Establish Secure channel and perform mutual authentication
16. Start Streaming (session information)
17. Start Streaming (session information)
18. Response ())
19. Response ()

Figure 6.5-6: ITF initiated Unicast Session Modification

- In steps 9-11, the response including the addressing information is relayed back to the Authentication and Session Management FE.
- Steps 12-13 are optional and are only applicable for managed networks. In these steps, based on the response received in step 9, the Authentication and Session Management FE verifies with the Network Resource Controller/Admission Control FE the availability of necessary network resources to handle the requested content ,.
- In step 14, the Authentication and Session Management FE forwards the response to the ITF.
- Step 15 is optional. In this step, a secure channel is established between the ITF and the Content Delivery Control function. This allows the CC function to authenticate the ITF before actual streaming the content. (Please refer to section Appendix A for more information.)
- In steps 16-19, the ITF requests streaming of the content. Notice that the streaming control signalling is proxied through the CC function to the CDF to prevent unauthorized access.

6.4.2.2 Server Initiated Unicast Session

Figure 6.5-7 shows a typical call flow for a new unicast session generated from a CC function towards a user who is already engaged in another unicast session. Below is a brief description of the steps that occur in this process:

The sequence is triggered by an action from the server. The server may have learnt somehow that a user is engaged in a session and decides to send an advertisement to the target user.

- In step 1, the advertising server sends a session initiation request to the Authentication and Session Management FE.
- In steps 2-3, the Authentication and Session Management FE performs admission control reservation for the new session. This step is optional for a managed network.
- In step 4, the request is forwarded to the IPTV Control where it is authorized based on the user profile stored there or fetched, if needed.
- In step 5, 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 FE is always in the signalling path and retains state information for all ongoing unicast sessions. In this case, the IPTV Control FE decides to initiate a new unicast session for the target user.
- In step 6, the Authentication and Session Management FE commits the reserved resources for the new session. This step is optional for a managed network.
- In step 7, the response is returned to the Authentication and Session Management FE.
- In step 8, the session initiation request arrives at the ITF which is currently rendering another stream.

In step 9-12, the ITF accepts the incoming request, and the response is forwarded to the CC FE, which can now initiate the stream from the CDF.

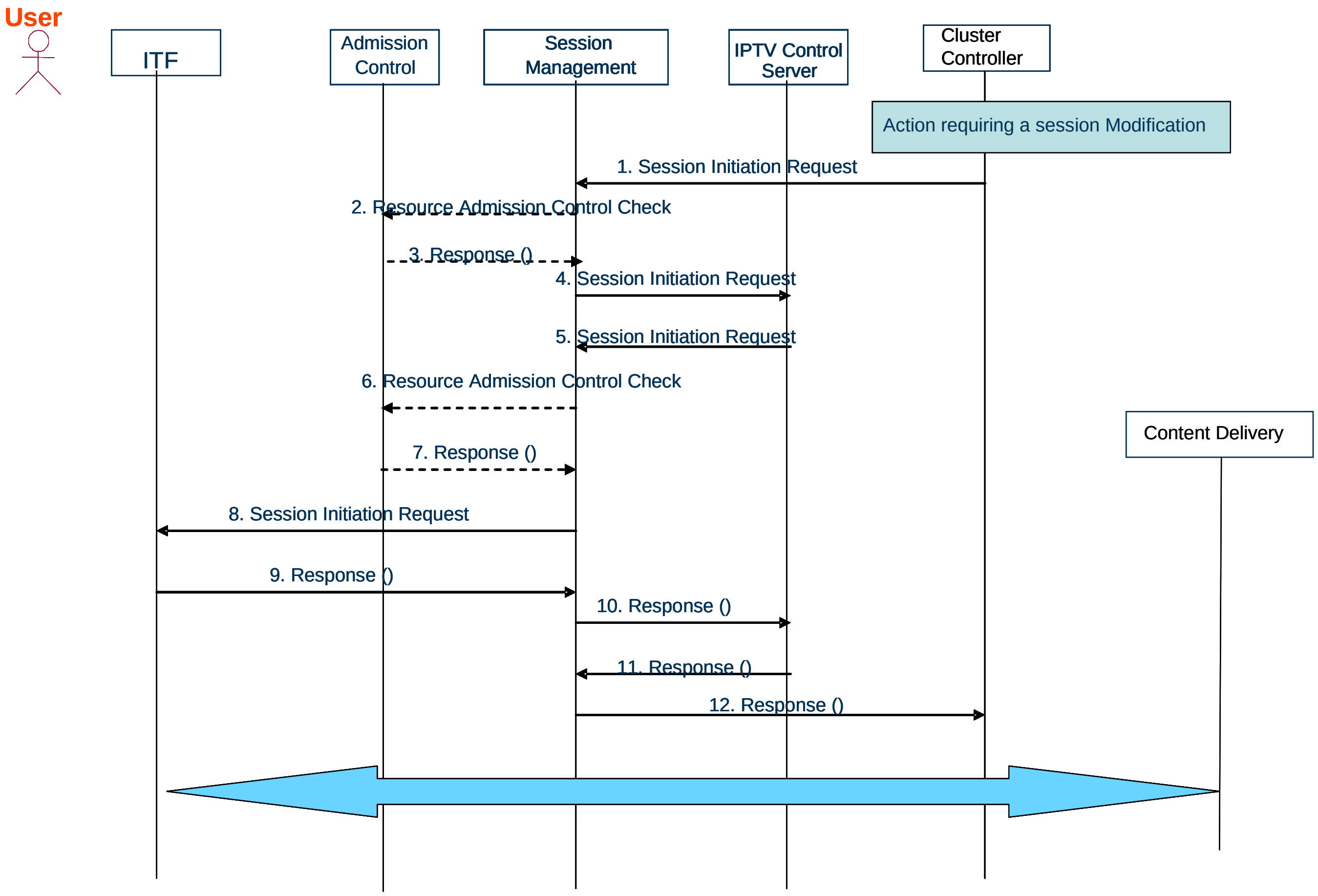

User
ITF
Admission Control
Session Management
IPTV Control Server
Cluster Controller
Action requiring a session Modification
1. Session Initiation Request
2. Resource Admission Control Check
3. Response ()
4. Session Initiation Request
5. Session Initiation Request
6. Resource Admission Control Check
Content Delivery
7. Response ()
8. Session Initiation Request
9. Response ()
10. Response ()
11. Response ()
12. Response ()

Figure 6.5-7: Network initiated unicast session modification

6.4.3 Session Teardown (managed model)

Figure 6.5-8 shows a typical call flow for a unicast session tear down. ".

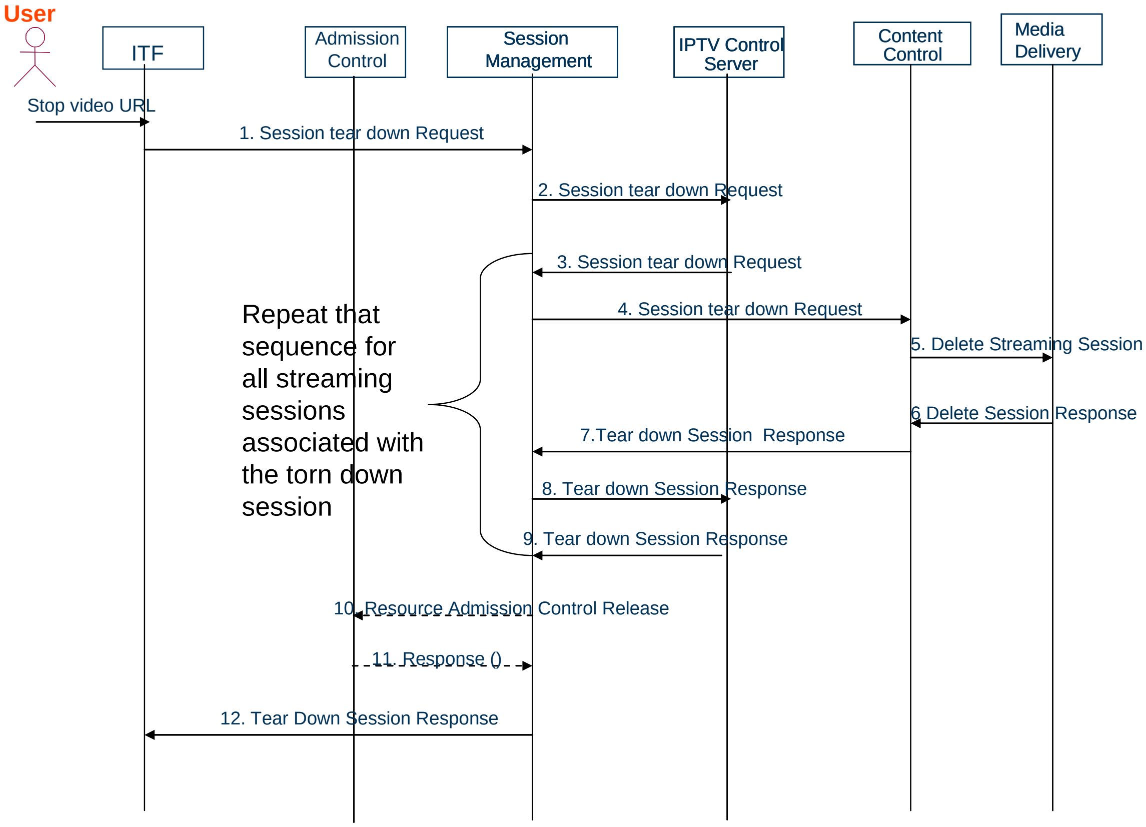

User
ITF
Admission Control
Session Management
IPTV Control Server
Content Control
Media Delivery
Stop video URL
1. Session tear down Request
2. Session tear down Request
3. Session tear down Request
4. Session tear down Request
5. Delete Streaming Session
6 Delete Session Response
7.Tear down Session Response
8. Tear down Session Response
9. Tear down Session Response
10. Resource Admission Control Release
11. Response ()
12. Tear Down Session Response
Repeat that sequence for all streaming sessions associated with the torn down session

Figure 6.5-8: Service Session tear down call flow

It is assumed that a Service Session and one or more associated Content delivery session 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 ITF requesting the termination of an ongoing unicast session which may or may not have an ongoing live stream.

- Signal 1: the ITF sends a session tear down request to the Session Management function.
- Signal 2: the request is forwarded to the IPTV Control FE.
- Signal 3: 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 3-9 are repeated for each content delivery session associated with the service session
- Signal 4: the Authentication & Session Management functionality forwards the request to the target Cluster Controller function.
- Signal 5: the target Cluster Controller function locates the Content Delivery function for the session, and sends a request to terminate the streaming session.
- Signal 6: the Content Delivery Function responds successfully to the termination request.
- Signals 7-9: the response is proxied all the way to the Session Management functionality.

- Signals 10-11 are optional and are only applicable for managed networks. In these steps, the Authenitcation & Session Management FE requests the release of the resources allocated to the unicast session by communicating with the Network Resource Controller/Admission Control FE.
- Signal 12, the Authentication & Session Management functionality forwards the response to the ITF.

6.4.4 Unicast Session Management (unmanaged model)

Unicast session management for live streaming in an unmanaged 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 phase in section 6.2.2.2.

6.4.4.2 Purchase of content from Service Providers over unmanaged networks

This call flow shows the steps used to purchase service or content from an IPTV Service Provider accessed over an unmanaged network.

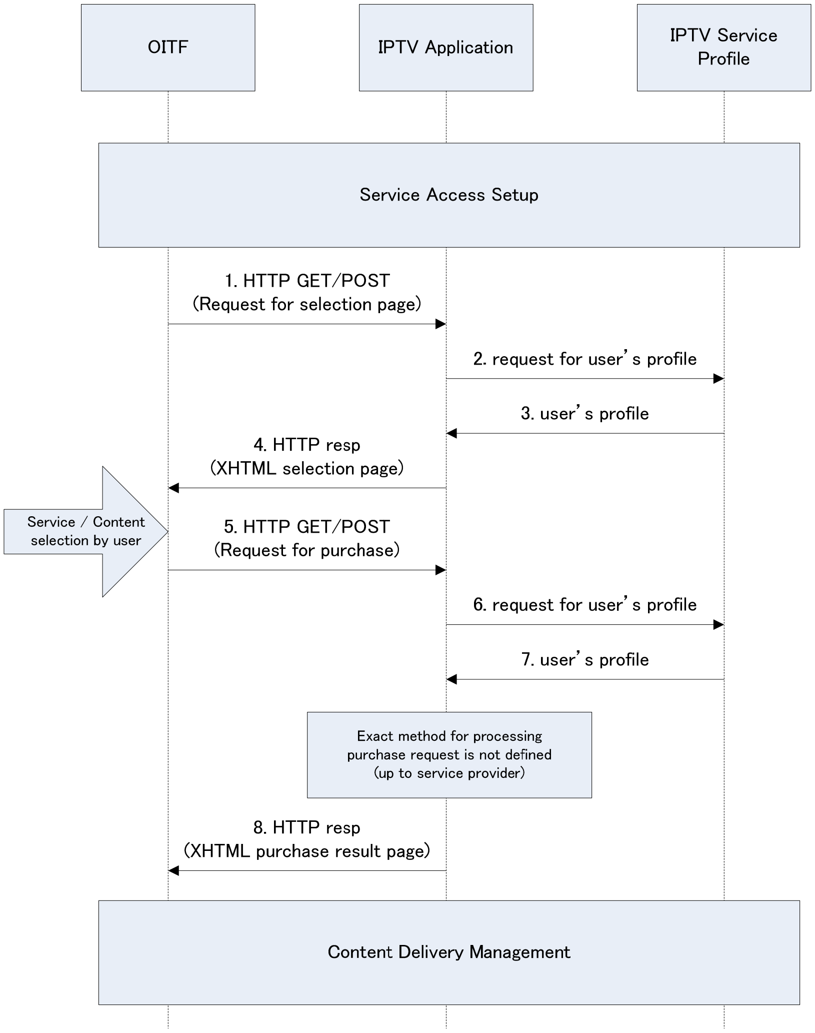

OITF
IPTV Application
IPTV Service Profile
Service Access Setup
1. HTTP GET/POST (Request for selection page)
2. request for user’s profile
3. user’s profile
4. HTTP resp (XHTML selection page)
Service / Content selection by user
5. HTTP GET/POST (Request for purchase)
6. request for user’s profile
7.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

Figure 4: 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.

- Signal 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 on OITF for presentation of a Content Guide to the user].

- Signals 2 and 3 involve the IPTV Application retrieving the user profile from the IPTV User Profile function, to customize the HTML page according to the user's profile. These steps are optional.

- Signal 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].

- Signal 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.

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

- Signal 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

This call flow shows the steps used to manage a unicast session in the case of an unmanaged network.

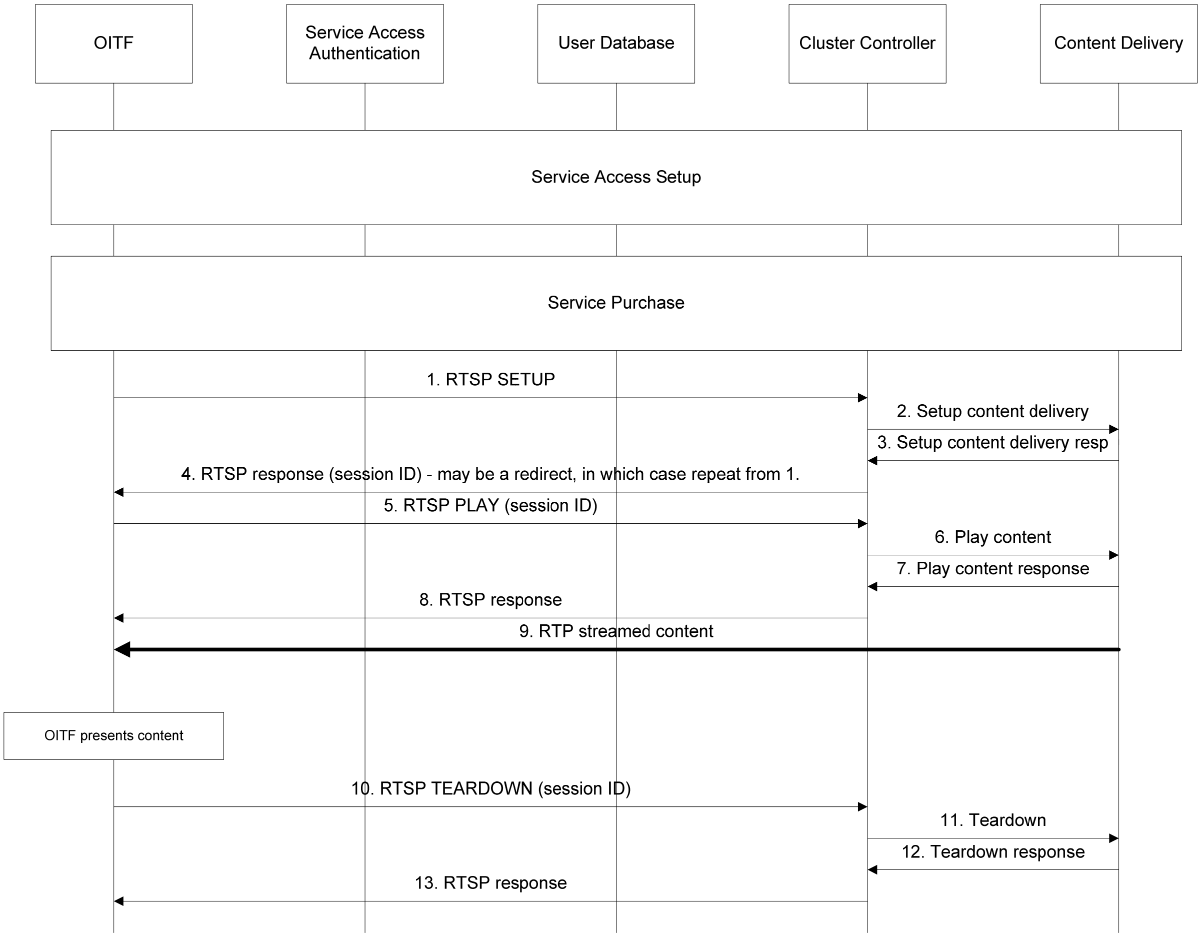


Figure 5: Call flow for unicast session management fro an unmanaged network

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

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

  Note: The SDP describing the requested media could be acquired from the content guide or using an RTSP DESCRIBE [Ref 20] – the exact method is left to the detailed protocol specifications.

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

- Signal 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.

- Signal 5 requests the Cluster Controller function to start streaming the content to the OITF.

- Signals 6 and 7 sets up the start the streaming of the content from the Content Delivery function.

- Signal 8 returns the status to the OITF.

- Signal 9 is the content being streaming from the Content Delivery functional entity to the OITF.

- Signal 10 will occur at some later time, when the OITF to longer wishes to receive the stream.
- Signals 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 Session management in the Residential network

The chapter shows the call flows within the residential network for accessing managed services. These call flows are complementary to those shown in other sections.

6.5.1 Unicast session setup

These call flows show the interactions in the residential network to set up, use and terminate a unicast session.

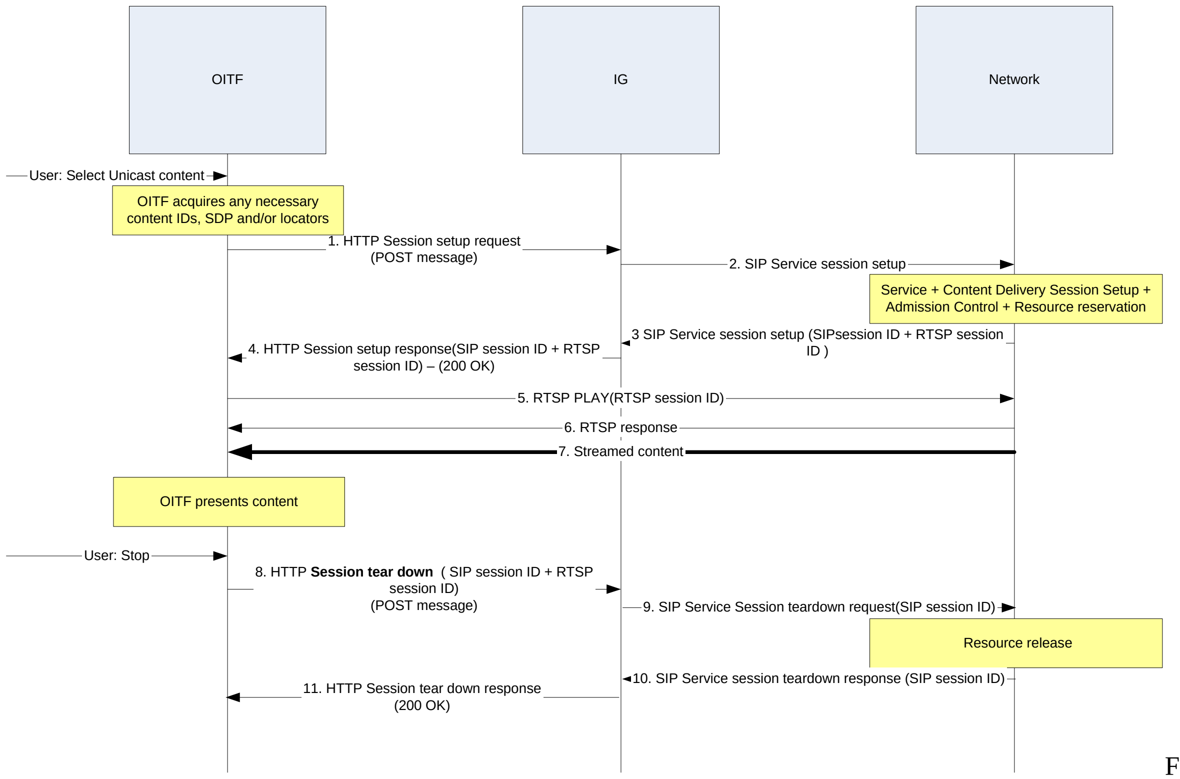

OITF
IG
Network
User: Select Unicast content
OITF acquires any necessary content IDs, SDP and/or locators
1. HTTP Session setup request (POST message)
2. SIP Service session setup
Service + Content Delivery Session Setup + Admission Control + Resource reservation
3 SIP Service session setup (SIPsession ID + RTSP session ID)
4. HTTP Session setup response(SIP session ID + RTSP session ID) – (200 OK)
5. RTSP PLAY(RTSP session ID)
6. RTSP response
7. Streamed content
OITF presents content
User: Stop
8. HTTP **Session tear down** (SIP session ID + RTSP session ID) (POST message)
9. SIP Service Session teardown request(SIP session ID)
Resource release
10. SIP Service session teardown response (SIP session ID)
11. HTTP Session tear down response (200 OK)

Figure [XXX]: Call flow for unicast session setup within the residential network

The following steps explain the call flow in detail.

- Via the OITF, the user selects an item of content from the content guide,..
- Signal 1 an HTTP require from the OITF to the IG requests the IG sets up the service delivery session,. This message includes the necessary information needed for the IG set up the service session.
- Signals 2 and 3 show the IG setting up the service session as required for the unicast service, as described in section [XXX]. This includes the selection of a Cluster Controller in the network to handle the content delivery session.
- Signal 4 returns the result of the service session setup to the OITF, including an RTSP session ID and an SDP file with the parameters for the stream, including the address of the Cluster Controller to be used for the content delivery session.
- Signals 5 to 7 show the RTSP PLAY command being sent from the OITF to the Cluster Controller, a response being returned, and content streaming beginning, as shown in section [XXX].

- The user requests the OITF to stop the content presentation.
- Signal 8 from the OITF requests the IG to terminate the content delivery and service sessions.
- Signals 9 to 11 terminate the content delivery and service sessions in the network and return a response to the OITF.

6.6 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 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;

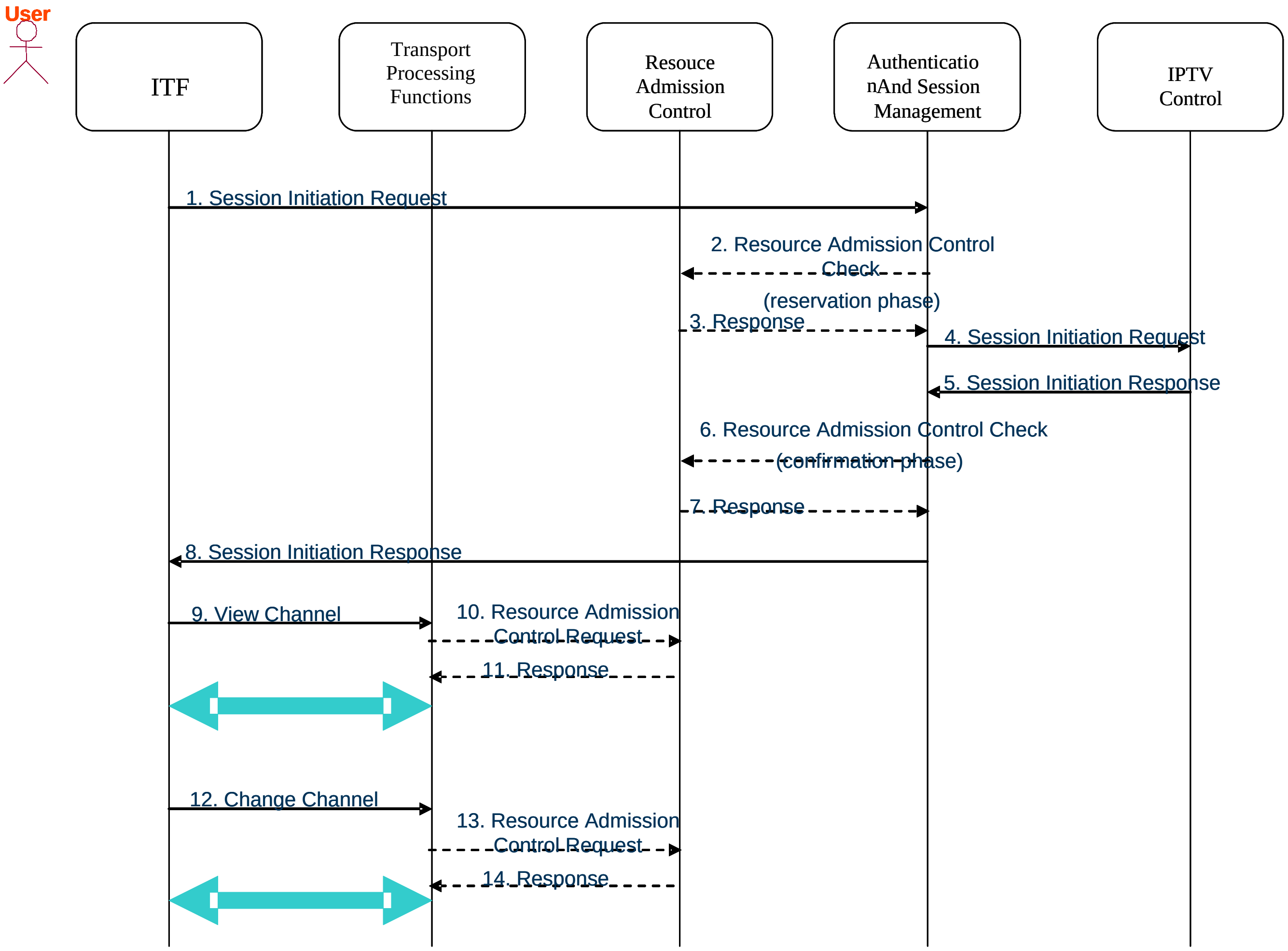
- the reserved subscriber resources (last mile) are released when conditions for such a release present themselves (the user stops watching scheduled content TV and switches to CoD, the TV is powered off, etc.);

- 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.

6.6.1 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.

The next figure shows an informational flow for the scheduled content session set-up.


User
ITF
Transport Processing Functions
Resouce Admission Control
Authenticatio nAnd Session Management
IPTV Control
1. Session Initiation Request
2. Resource Admission Control Check
(reservation phase)
3. Response
4. Session Initiation Request
5. Session Initiation Response
6. Resource Admission Control Check
(confirmation phase)
7. Response
8. Session Initiation Response
9. View Channel
10. Resource Admission Control Request
11. Response
12. Change Channel
13. Resource Admission Control Request
14. Response

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

1. The ITF sends a session initiation request to the Authentication and Session Management, 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 forwards the request to the IPTV Control, which verifies that the user is authorized for the service and verifies 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. The response for the admission control request is returned.

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

9/12. The ITF sends a request to Transport Processing Functions to view/change the channel.

10/11/13/14. (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),

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.

6.6.2 Scheduled Content service session teardown procedure

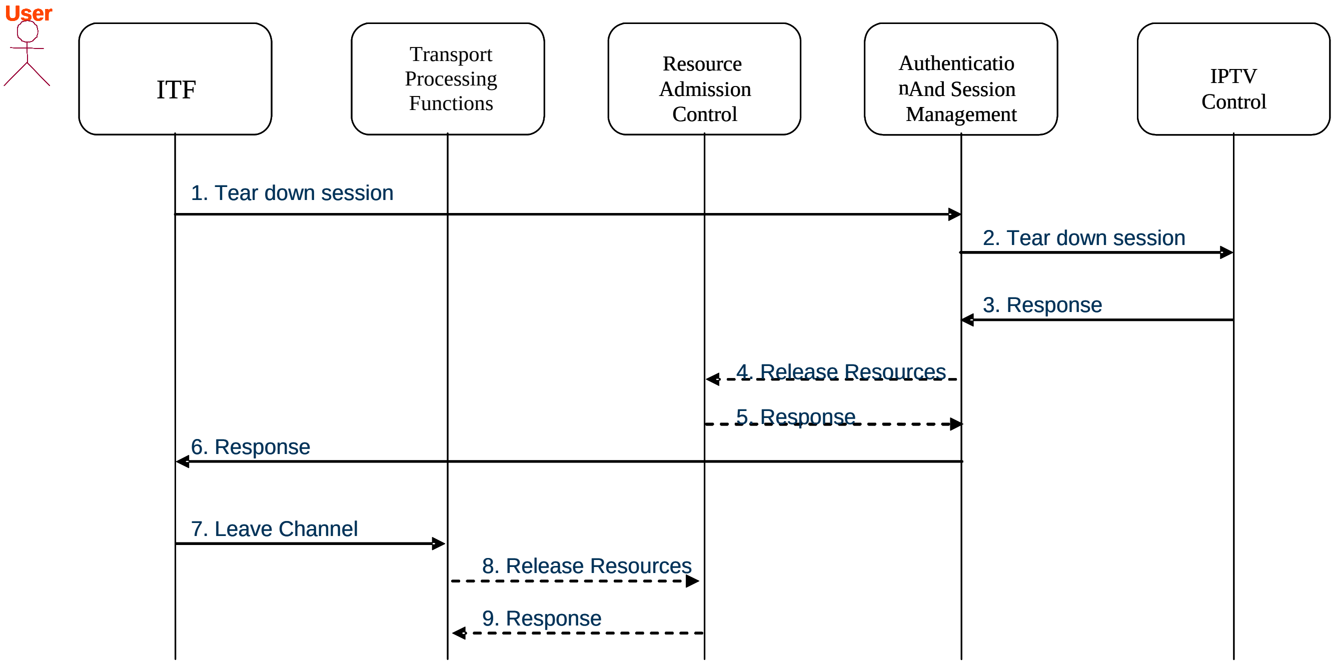


Figure 3: Scheduled Content service Session Teardown Call Flow

Figure 3 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 session tear down request to the Authentication & Session Management Functionality.

2. The Authentication & Session Management Functionality forwards the request to the IPTV Control FE.

3. The IPTV Control FE updates its internal states, if required, and sends a 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 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.

[Note: Is it necessary to move steps 7, 8, 9 before step one, in order to be sure to release resources before doing step 4?]

6.7 Push Content session management procedures (managed networks)

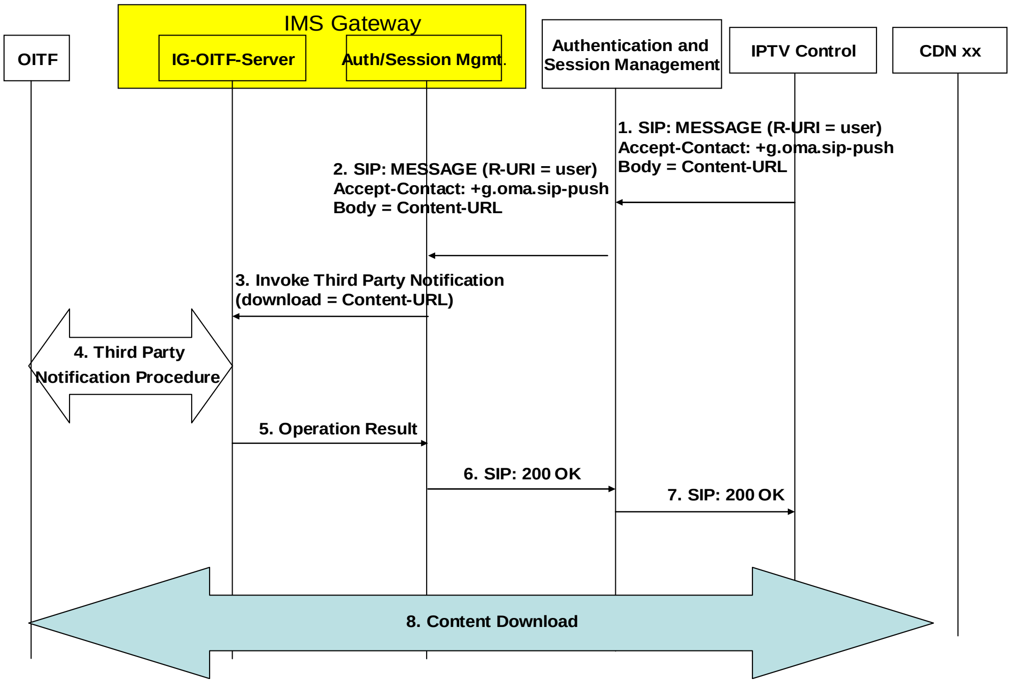
The Push procedure defines a mechanism for supporting Service Provider initiated IPTV services as, for example, Push CoD.

The CoD can be pushed to an OITF, asynchronously, during the period the user is registered with the IPTV domain. The Push 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.

The figure below depicts an informational flow for the Push procedure, applied to the Push CoD service.

Push Procedure


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

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; 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 and Session management module
3. The Auth/Session Mgmt. module, invokes the third party notification functionality in the IG-OITF-SERVER server.
4. The IG-OITF-SERVER server starts the notification procedure in the OITV 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 CE 2014 operations so that the OITF can displays the appropriate message; more in details:
  - 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”.
  - OITF, receives the notification message and load, from IG_RUI, the content referred by the “notification content”. In this case the “notification content” contains a scripting object (which includes the *Content-URI*) that triggers, on OITF, the download of the content from the CDN.
  - OITF sends the response to IG-OITF-SERVER after the “notification content” loading;
- UPnP GENA

5. The IG-OITF-SERVER server reports the Operation Result to the Auth/Session Mgmt. module on 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.

7. Interworking between IPTV and Communication Services

7.1 Caller ID

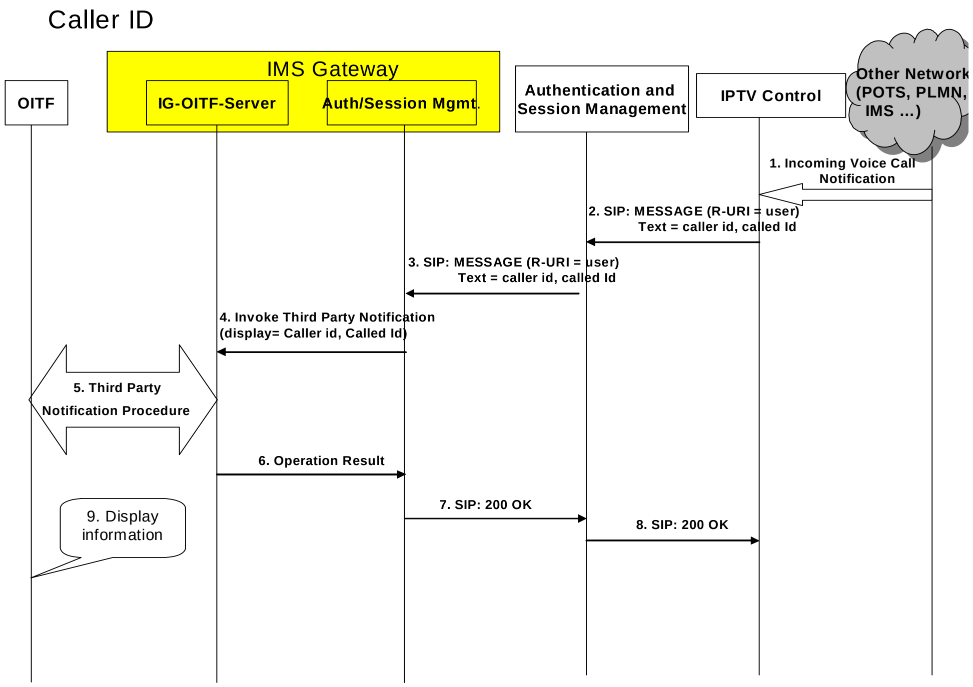
The Communication Service Caller ID feature allows the display on an OITF of the Caller Id for an incoming voice call. When a user receives a voice call, information related to the Caller ID is sent to the IPTV Control from the network managing the call. Via session management procedures, the OITF is 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 21] (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 IPTV Control server, 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 IPTV Control Server is out of scope of this specification

The next figure shows an informational call flow for the Caller ID communication service.


Caller ID
IMS Gateway
OITF
IG-OITF-Server
Auth/Session Mgmt.
Authentication and Session Management
IPTV Control
Other Network (POTS, PLMN, IMS …)
1. Incoming Voice Call Notification
2. SIP: MESSAGE (R-URI = user) Text = caller id, called Id
3. SIP: MESSAGE (R-URI = user) Text = caller id, called Id
4. Invoke Third Party Notification (display= Caller id, Called Id)
5. Third Party Notification Procedure
6. Operation Result
7. SIP: 200 OK
8. SIP: 200 OK
9. Display information

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

As a precondition, the User must be registered via the Authentication and Session Management (IMS) prior to the call flow.

1. A network (POTS, PLMN, IMS …) notifies the IPTV Control 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 IPTV Control generates and sends a SIP MESSAGE (that includes the *caller Id*, the *called Id*, additional information) towards the IPTV User Authentication and Session Management;

3. The SIP MESSAGE is proxyed to the IMS Gateway, where it is intercepted by the Authentication and Session management module;

4. The Auth/Session Mgmt. module invokes the third party notification functionality in the IG-OITF-SERVER server.

5. The IG-OITF-SERVER server 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 CE 2014 operations so that the OITF can displays 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_RUI, 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;

        - Issue of UPnP GENA

6. The IG-OITF-SERVER server reports the Operation Result to the Auth/Session Mgmt. module on IMS Gateway;

7-8 The response for the MESSAGE request is forwarded to the IPTV Control via Authentication and Session Management;

9. The OITF displays the information on the screen.

7.2 Messaging

The Communication service Messaging allows a user to send/receive textual messages to/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 domain.
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 22] 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 23]

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

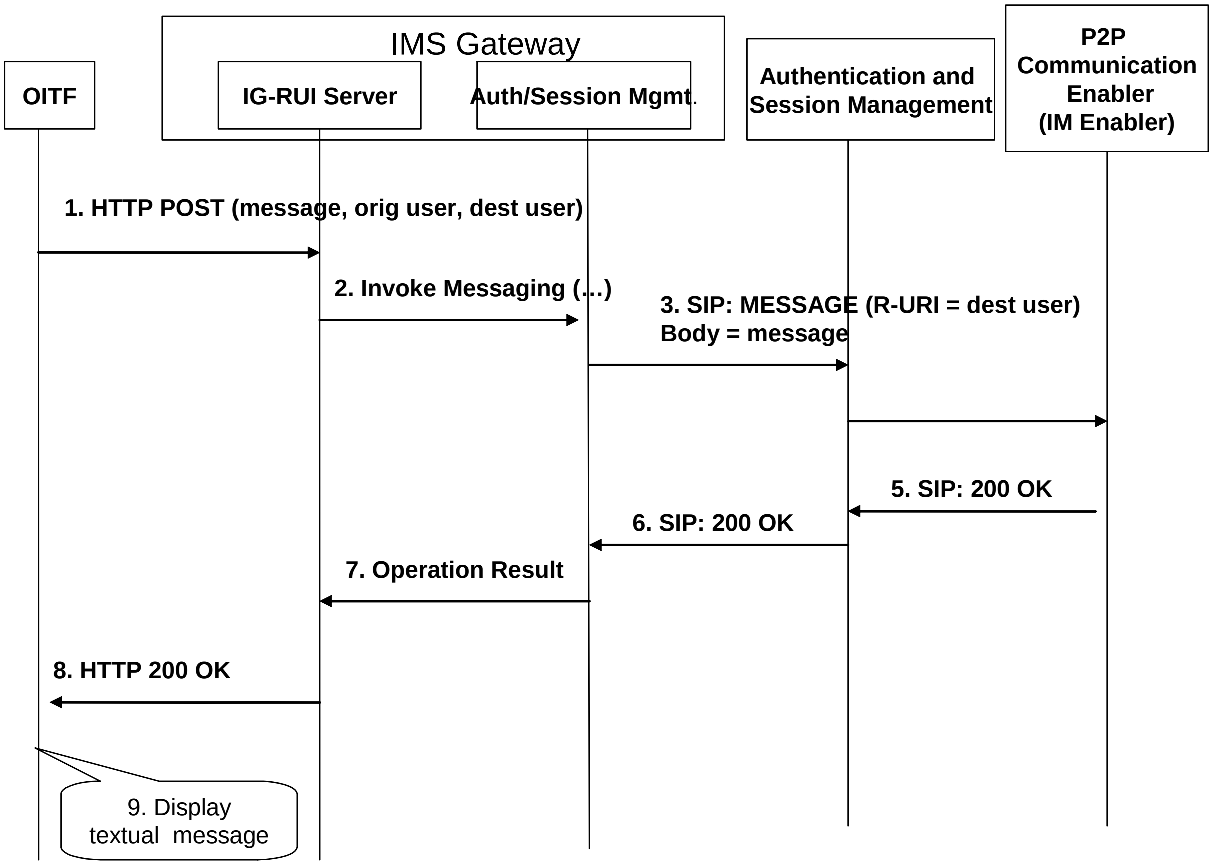
- A DA-DLE application (HTML + ECMAscript [Ref 24]) downloaded to the OITF

Or

- A native application on the OITF

7.2.1 Outgoing messaging

The figure below shows an example of outgoing messaging communication service, followed by a brief description of the flow.

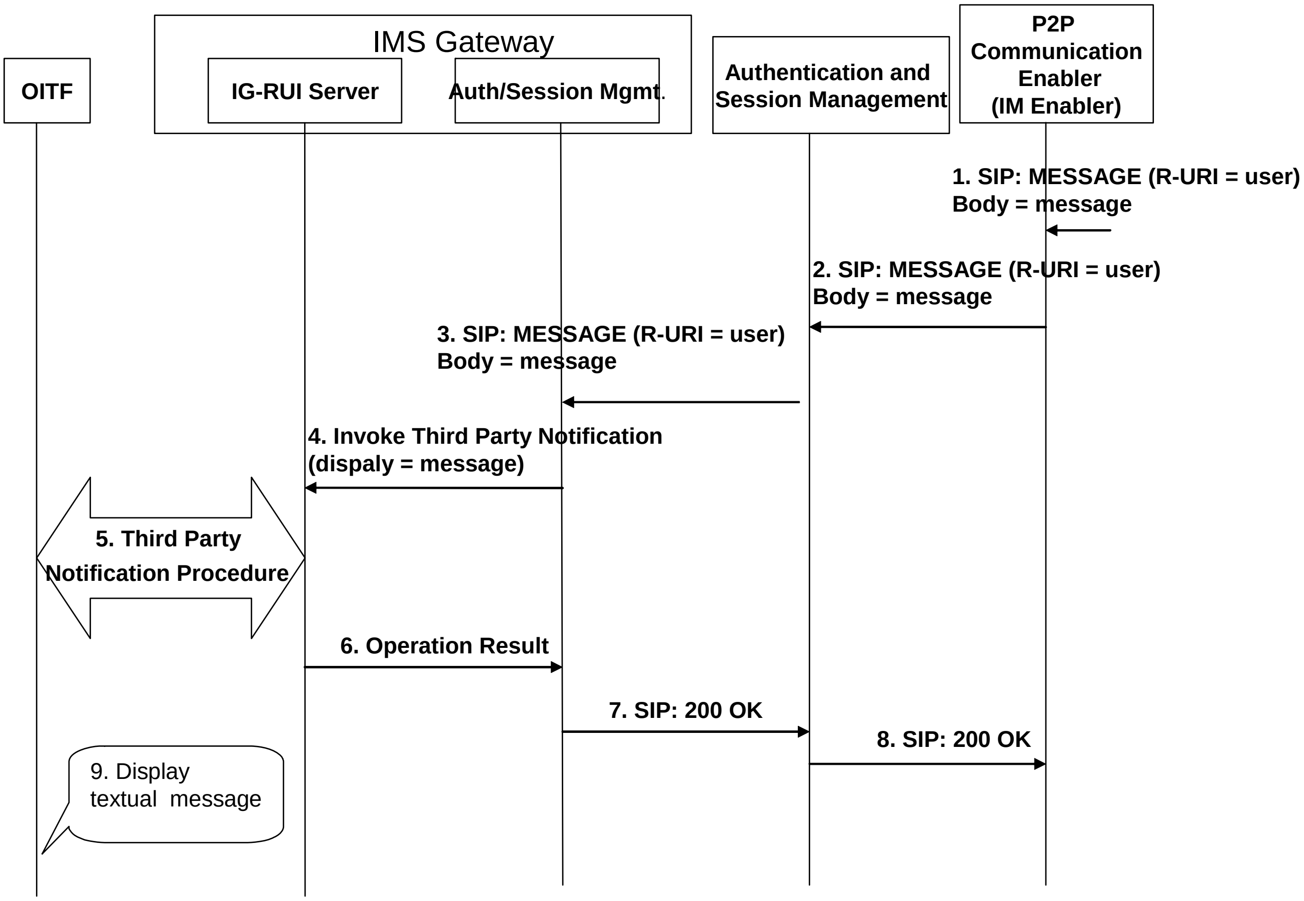

IMS Gateway
OITF
IG-RUI Server
Auth/Session Mgmt.
Authentication and Session Management
P2P Communication Enabler (IM Enabler)
1. HTTP POST (message, orig user, dest user)
2. Invoke Messaging (…)
3. SIP: MESSAGE (R-URI = dest user) Body = message
5. SIP: 200 OK
6. SIP: 200 OK
7. Operation Result
8. HTTP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

1. A user logged on an OITF wants to send a text message. The OITF sends an HTTP POST message including the text to be sent, the originating user and the receiving user (or list of users) to the IG-OITF server.
2. The IG-OITF server intercepts the HTTP request and invokes the IG Auth/Session Mgmt function to send the text.
3. The Auth/Session Mgmt. module composes a SIP MESSAGE (that includes the textual message) and sends it to the user's home Authentication and Session Management.
4. Based on the filter criteria of the user, the SIP MESSAGE is forwarded to the IM Enabler function; the IM Enabler function is in charge to delivery the textual message to the final receiver or the users in the list;
5. A 200 OK is received as a response from the terminating network;
6. The 200 OK is proxyed to 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

The figure below shows an example of incoming messaging communication service, followed by a brief description of the flow.

.


IMS Gateway
OITF
IG-RUI 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 (dispaly = message)
5. Third Party Notification Procedure
6. Operation Result
7. SIP: 200 OK
8. SIP: 200 OK
9. Display textual message

7. A text message has been sent to the user; the message arrives to the IM Enabler function, responsible for managing the message delivery to the final receiver (or the users belonging to list);
8. 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;
9. The SIP MESSAGE is proxyed to the user IMS Gateway, where it is intercepted by the IG Auth/Session Mgmt function;
10. The IG Auth/Session Mgmt function invokes the third party notification functionality in the IG-OITF server.
11. The IG-OITF server starts the Third Party Notification Procedure. In particular the IG-OITF sends the appropriate CE 1024 operations so that the OITF displays the appropriate message. In more detail:
    - The IG-OITF 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 the IG_RUI, 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.
    - OITF sends the response to the IG-OITF after the “notification content” loading;

12. The IG-OITF server reports the Operation Result to the IG Auth/Session Mgmt function on the IMS Gateway;

7-8 Finally, the response for 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 an 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.

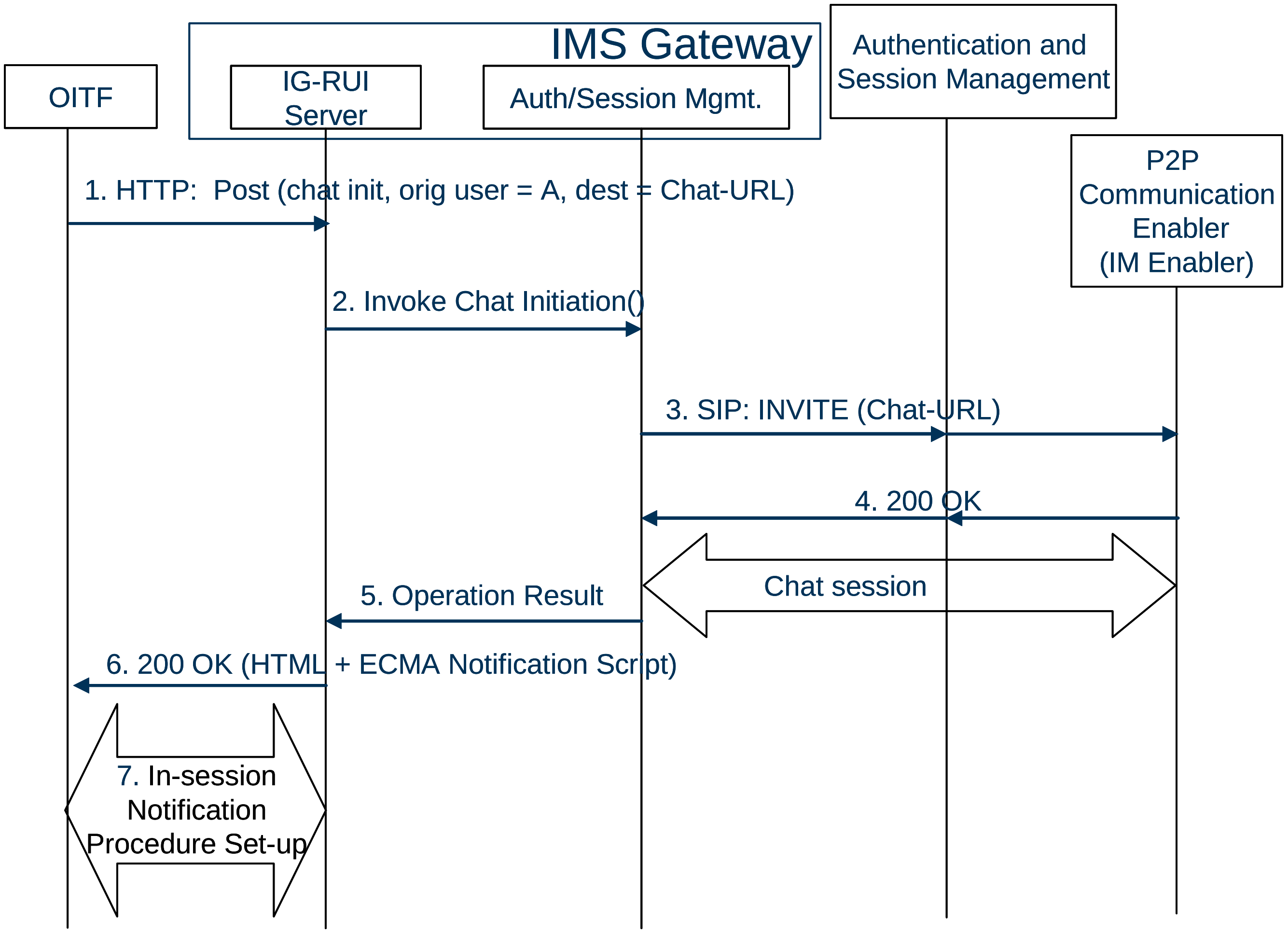
The messages are sent/received within a communication context; the state of the communication context is stored in the IPTV Solution.

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) allowing the exchange of Instant Messaging messages between users in near real-time, based on the IETF SIP protocol [RFC3261] 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 23]

The figure below 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 the [Note: include reference to the paragraph describing Presence – Presence template produced by the IG].

7.3.1 Chatting session set up


IMS Gateway
OITF
IG-RUI 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. 200 OK
Chat session
5. Operation Result
6. 200 OK (HTML + ECMA Notification Script)
7. In-session Notification Procedure Set-up

1. A user logged on 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. 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).

4. 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

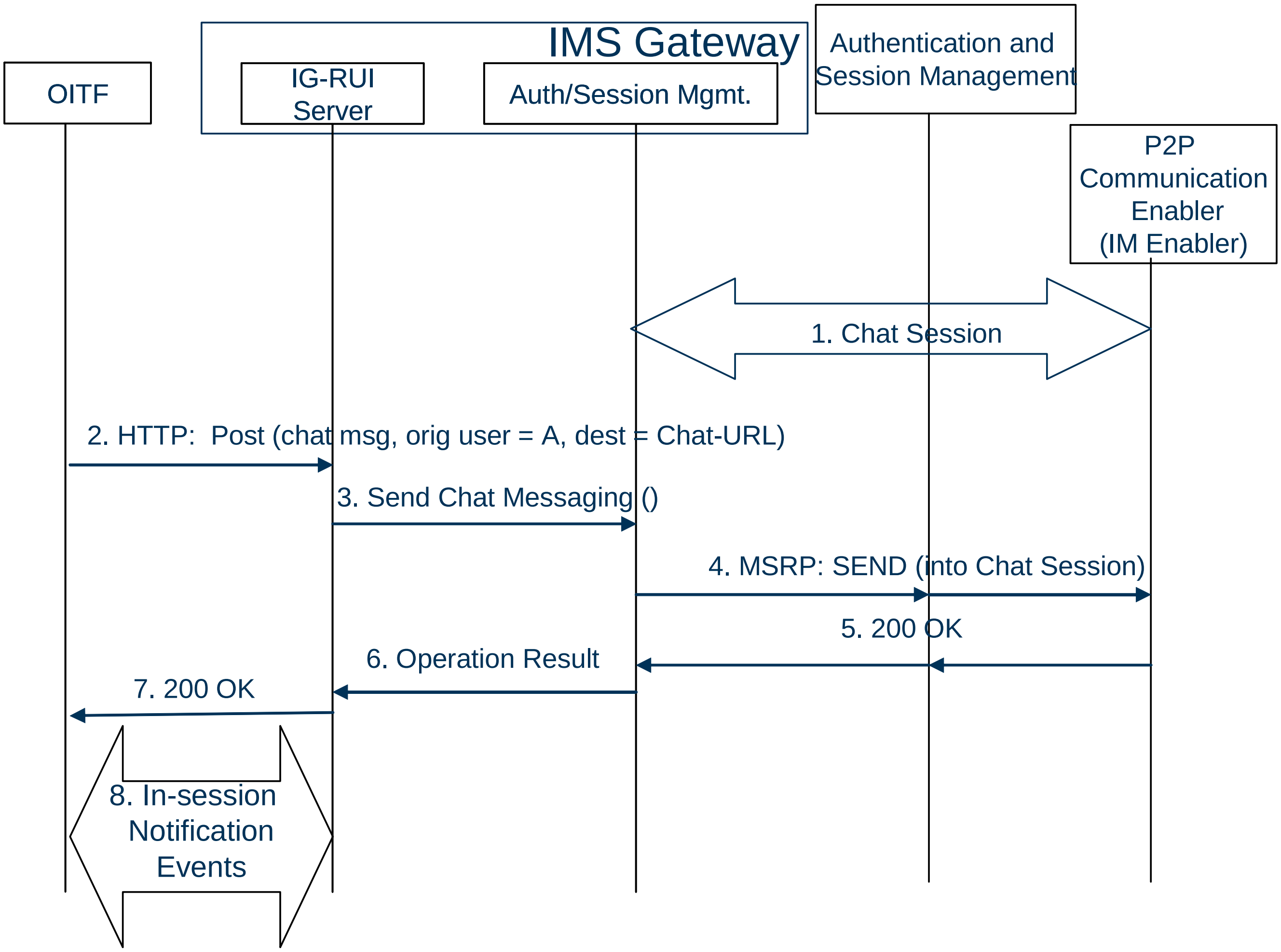
5. The IG Auth/Session Mgmt function sends the operation result to the IG-OITF server;

6. 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.

7. The OITF sets up an In-Session Notification Procedure (XML HTTP request or Persistent TCP Connection Mode) with the IG-OITF. The IG-OITF 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 Chatting outgoing message

The figure below shows an example of chatting outgoing message, followed by a brief description of the flow.


IMS Gateway
OITF
IG-RUI 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. 200 OK
6. Operation Result
7. 200 OK
8. In-session Notification Events

1. A user logged on an OITF has already established a chat session (for details see **Error! Reference source not found.**) 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. The IG Auth/Session Mgmt function composes a MSRP message (that includes the text message) and sends it, in the chat session, to the user’s home network Authentication and Session Management FE. The MSRP message is proxied to the IM Enabler function.

5. A MSRP 200 OK is received as a response from the IM Enabler function and it is proxied to IMS Gateway;

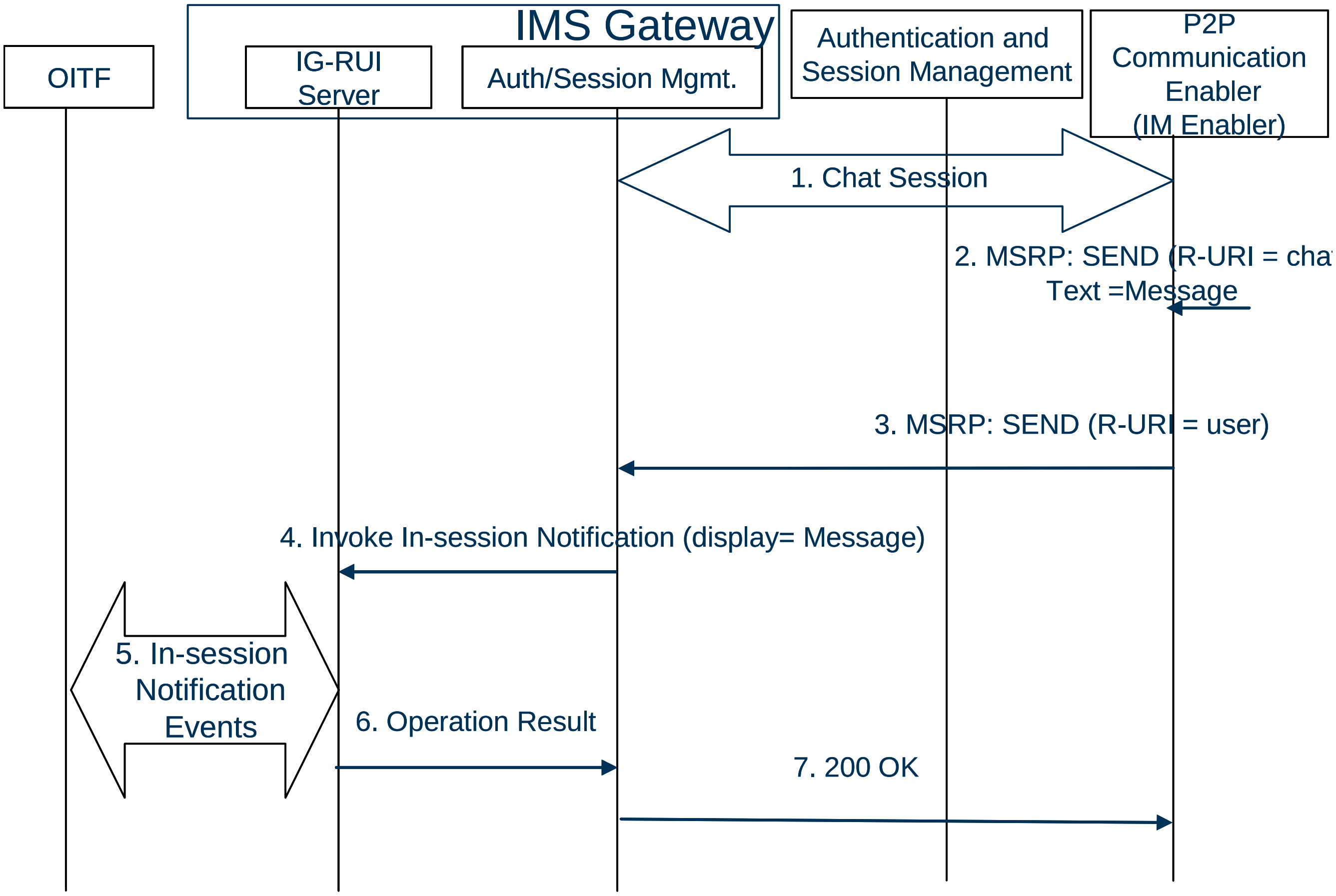
6. The IG Auth/Session Mgmt sends the operation result to the IG-OITF server.

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

8. IG-OITF server, if needed, performs the necessary CE-1024 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 Chatting incoming message

The figure below shows an example of chatting incoming message, followed by a brief description of the flow.


IMS Gateway
OITF
IG-RUI Server
Auth/Session Mgmt.
Authentication and Session Management
P2P Communication Enabler (IM Enabler)
1. Chat Session
2. MSRP: SEND (R-URI = cha
Text =Message
3. MSRP: SEND (R-URI = user)
4. Invoke In-session Notification (display= Message)
5. In-session Notification Events
6. Operation Result
7. 200 OK

1. A user logged on an OITF has already established a chat session (for detail see par 2.1) with IPTV Control.
2. The IM Enabler function receives a MSRP SENT message (that includes the message to be delivered to the OITF) from another user in the chat session (identified by a Chat-URL) ;
3. The MSRP SEND message is proxyed via Authentication and Session Management to the user's IMS Gateway, where it is intercepted by the IG Auth/Session Mgmt function
4. The IG Auth/Session Mgmt function invokes the In-session Notification functionality in the IG-OITF server.
5. IG-OITF server performs the necessary CE-2014 operation so that the OITF displays the message to be delivered on the screen, using the In-Session Notification established earlier during the chat session set-up procedure. The IG-OITF server reports the Operation Result to the IG Auth/Session Mgmt function on the IMS Gateway;

6-7 Finally, the response for the MSRP SENT 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 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 procedure.

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, for example:

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

Figure 7.4-1 shows the mechanism proposed in order to allow an ITF to communicate Presence information. 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 (privacy preferences) as to which specific IPTV attributes to include in the Presence information that is made available to other users.

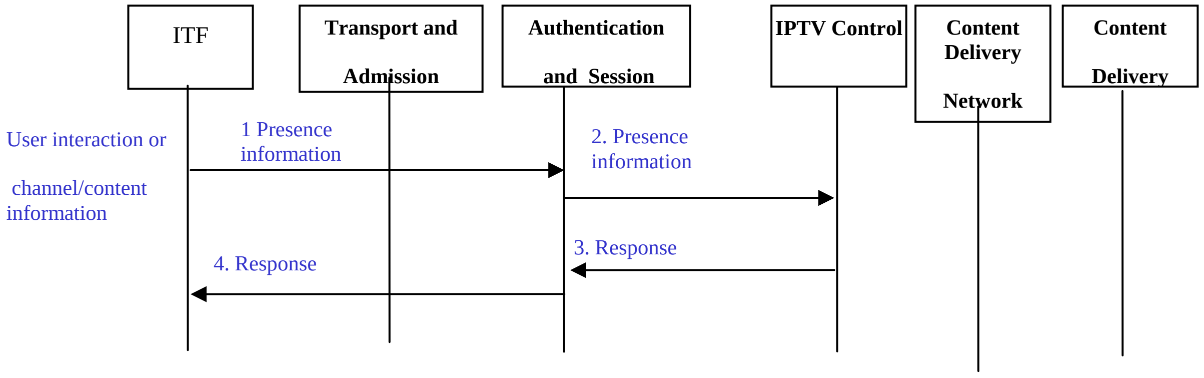


Figure 7.4-1 Call flow for sending Presence information to IPTV Control

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.

7.4.2 Presence Session Management Procedures

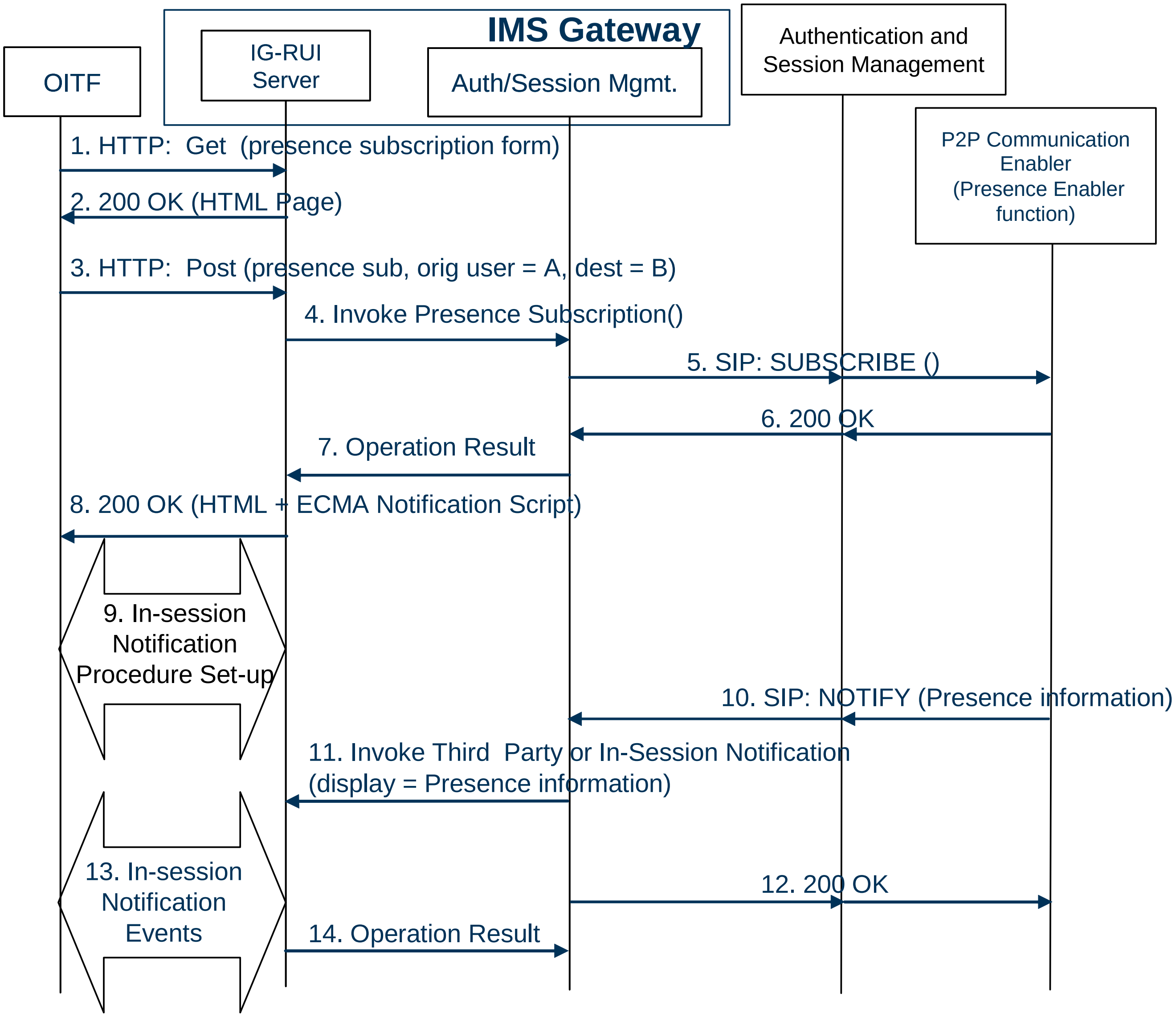
The Communication service. Presence. allows multiple users of an ITF to communicate their presence information inside an IPTV Service network. A user (A) can subscribe to the presence information of other users (B,C …) so that when one of these users change their Presence status user (A) will receive a notification for 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 22] 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 25]

The figures below show two examples of the use of the Presence service with IPTV.

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


IMS Gateway
OITF
IG-RUI Server
Auth/Session Mgmt.
Authentication and Session Management
P2P Communication Enabler (Presence Enabler function)
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. 200 OK
7. Operation Result
8. 200 OK (HTML + ECMA Notification Script)
9. In-session Notification Procedure Set-up
10. SIP: NOTIFY (Presence information)
11. Invoke Third Party or In-Session Notification (display = Presence information)
12. 200 OK
13. In-session Notification Events
14. Operation Result

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 for 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 IG Auth/Session Mgmt. function.

5. The IG Auth/Session Mgmt. function composes 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 200 OK is received as a response from the network

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, 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.

9. 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. .

10. The IG Auth/Session Mgmt. function receives a NOTIFY message that includes the Presence status.

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

12. The IG Auth/Session Mgmt. function responds to the NOTIFY with a 200 OK message

13. The IG-OITF Server performs the necessary in-session notification operation (CEA 2014) 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.

14. 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 [UNDER REVIEW]

In the **Scheduled Content** channel switching, 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 change 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 Solution 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 7.4-2 and Figure 7.4- provide examples of a signalling flow for channel switching, in the case of Client side and Server side load control.

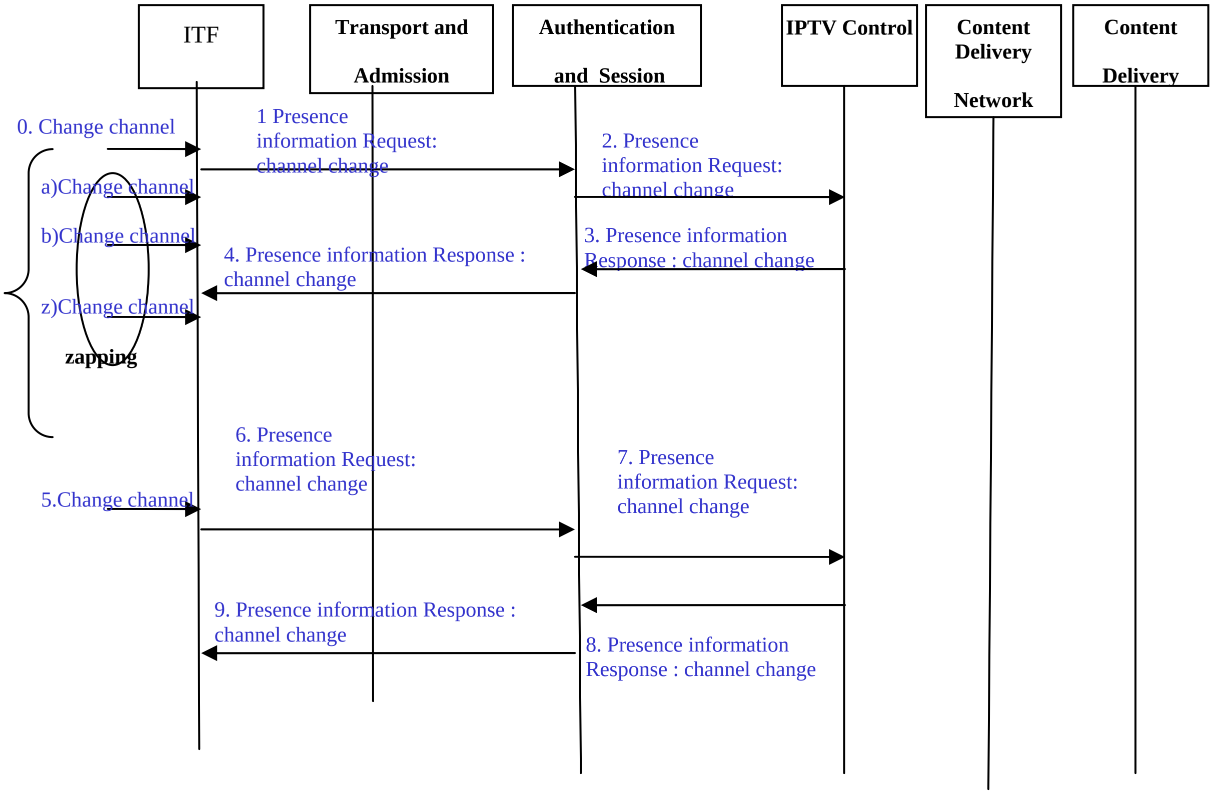

ITF
Transport and Admission
Authentication and Session
IPTV Control
Content Delivery Network
Content Delivery
0. Change channel
1 Presence information Request: channel change
2. Presence information Request: channel change
a)Change channel
b)Change channel
3. Presence information Response : channel change
4. Presence information Response : channel change
z)Change channel
zapping
6. Presence information Request: channel change
7. Presence information Request: channel change
5.Change channel
9. Presence information Response : channel change
8. Presence information Response : channel change

Figure 7.4-2: 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 is being watched.
(2) Authentication and Session Management routes the information to the IPTV Control.
(3) IPTV Control responds to the Inform channel change request.
(4) Authentication and Session Management routes the response to the ITF.

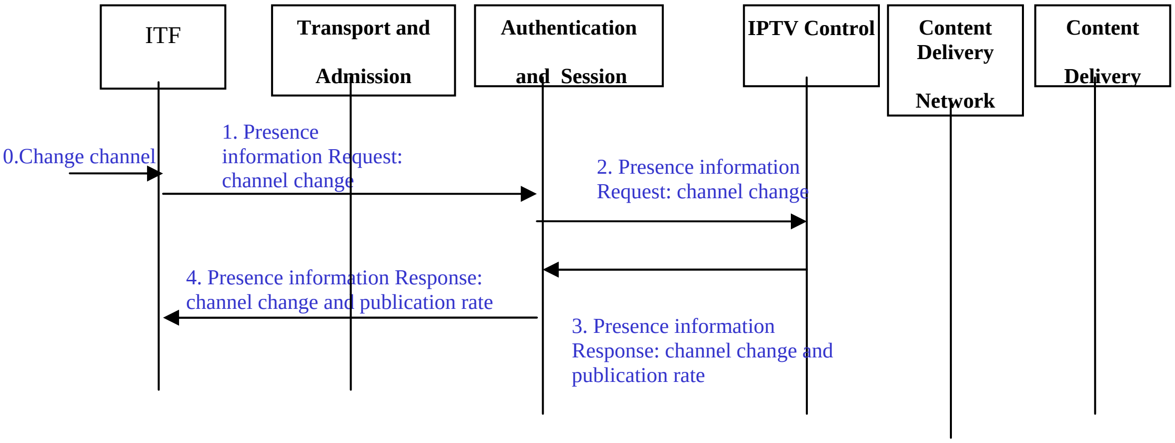

ITF
Transport and Admission
Authentication and Session
IPTV Control
Content Delivery Network
Content Delivery
0.Change channel
1. Presence information Request: channel change
2. Presence information Request: channel change
4. Presence information Response: channel change and publication rate
3. Presence information Response: channel change and publication rate

Figure 7.4-3: Scheduled Content (Broadcast TV) channel switching: Server Side load control

(5) The ITF leaves a multicast channel and joins another multicast channel.
(6) The ITF sends information about which channel is being watched.

(7) The Authentication and Session Management FE routes the information to the IPTV Control.

(8) 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.

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

Appendix A. Compliance of Architecture to the Requirements

[UNDER REVIEW]

Appendix B. Proxy Description and Single-SignOn (Informative)

This section introduces single-sign on architecture defined for IMS, and known as the Generic Bootstrap Architecture (GBA) [Ref 26], and the role the authentication proxy.

B.1 Single Sign On Architecture Description

Figure C-1 depicts the proposed 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.

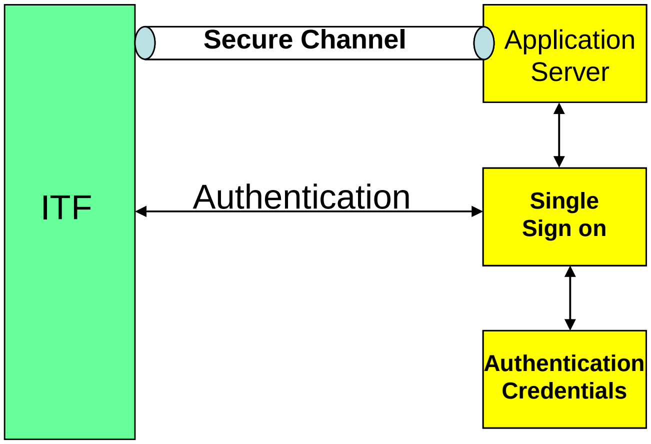


Figure C-1-: Single Sign-on Architecture

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 single sign-on FE.. Once successfully authenticated with the single sign-on FE, 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 single sign-on FE, 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 single sign-on FE. 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 user profile.

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

1. The ITF authenticates itself with the single sign-on FE 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 the ASs with whom it desires to communicate.
3. The single sign-on FE 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 single sign-on FE
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 single sign-on FE.

7. Mutual authentication is now completed and signalling exchange can start.

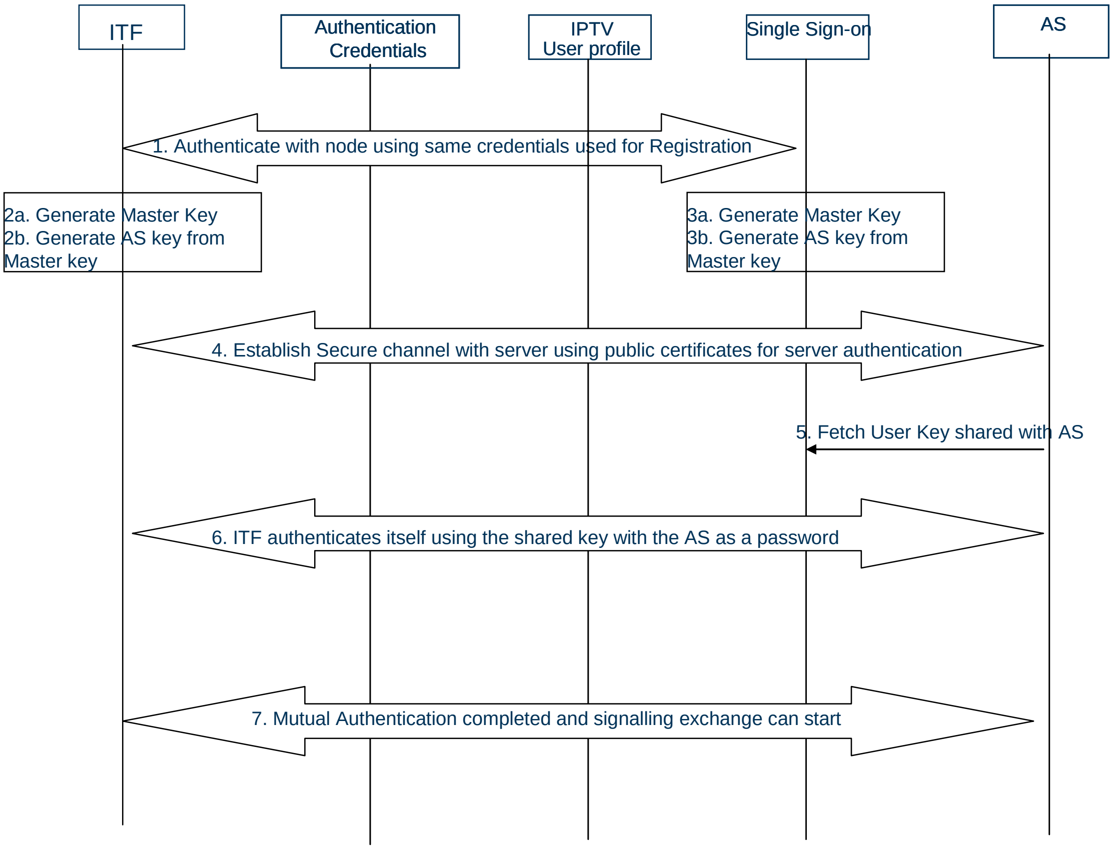

ITF
Authentication Credentials
IPTV User profile
Single Sign-on
AS
1. Authenticate with node using same credentials used for Registration
2a. Generate Master Key
2b. Generate AS key from Master key
3a. Generate Master Key
3b. Generate AS key from Master key
4. Establish Secure channel with server using 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 signalling exchange can start

Figure C-2 : Single Sign-on Call Flow

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

The procedure presented on Figure C-2**Error! Reference source not found.** 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 C-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 takes over the AS address through DNS lookup.

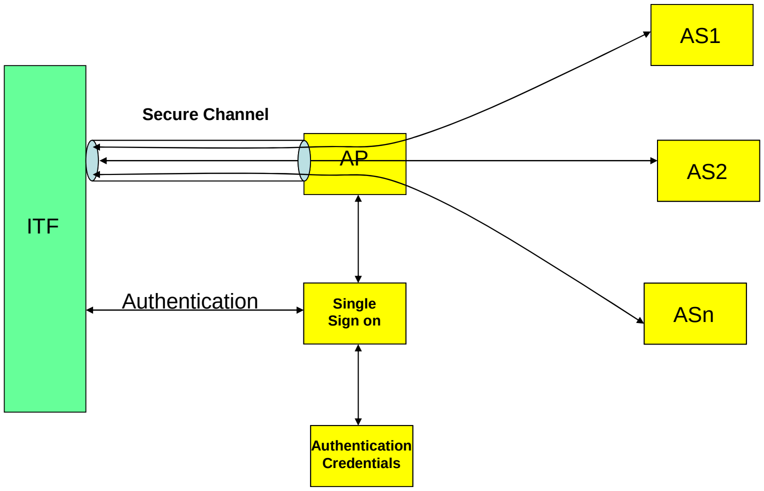


Figure C-3 : Authentication Proxy and Single Sign-on Architecture

Appendix C. Content Delivery Network Architecture description and Call flows (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 doesn't 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 D-1.

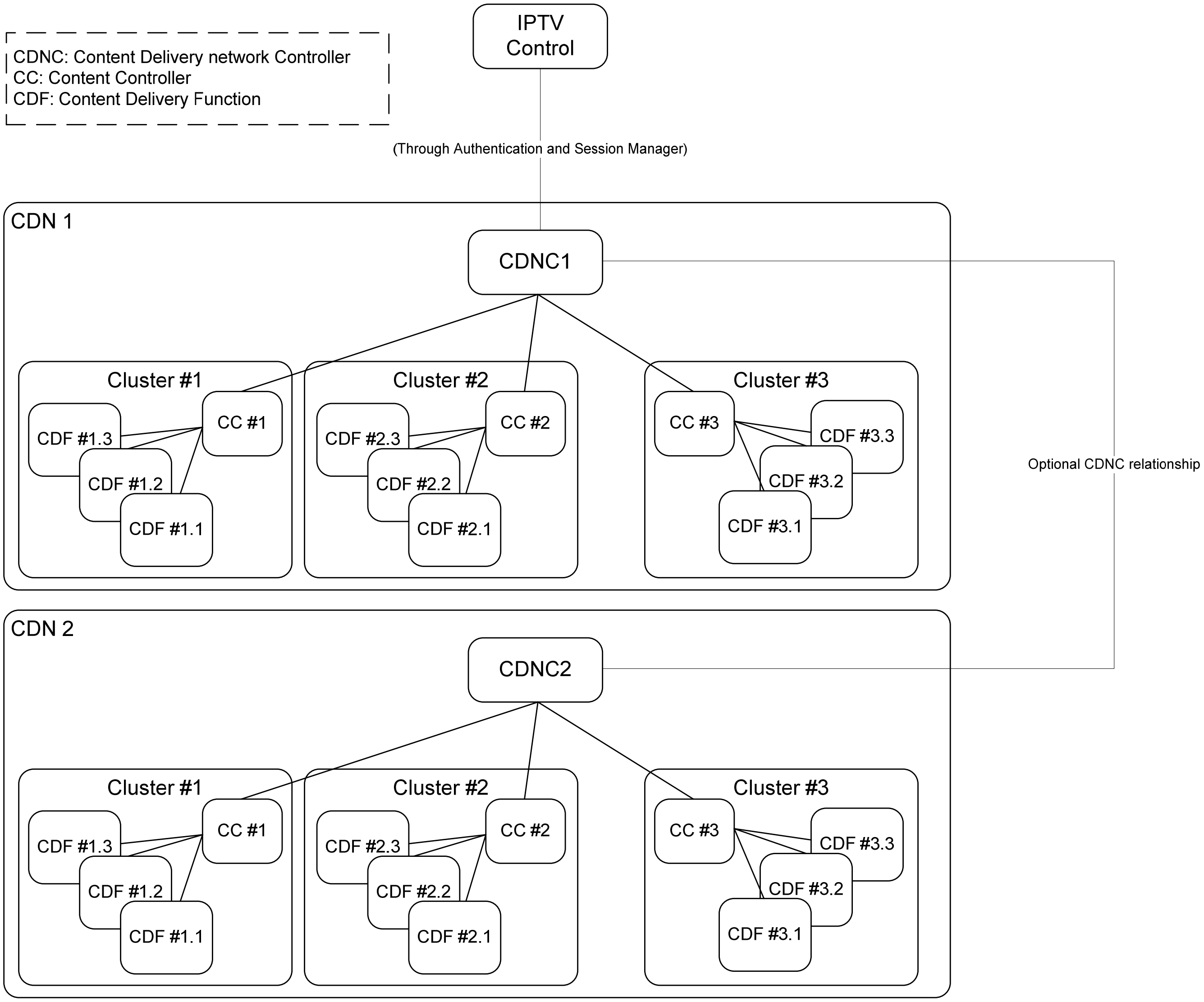


Figure D-1: Relationship between IPTVC/CDNC/CC/CDF

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 IPTVC, 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 concerns, 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 to establish the Content Delivery Session and control its progress
  - a Content Delivery Session Transfer Plane : this allows to deliver 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 ceck section 6.4.2 for more information.

The IPTVC, 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 **Error! Reference source not found.**). the right CDN controller's choice could be based on:
  - Video Content Selection Parameters
  - CDNC's organisation (**Error! Reference source not found.** outline a few examples of such an organization)
  - Search and discovery algorithms (e.g P2P 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

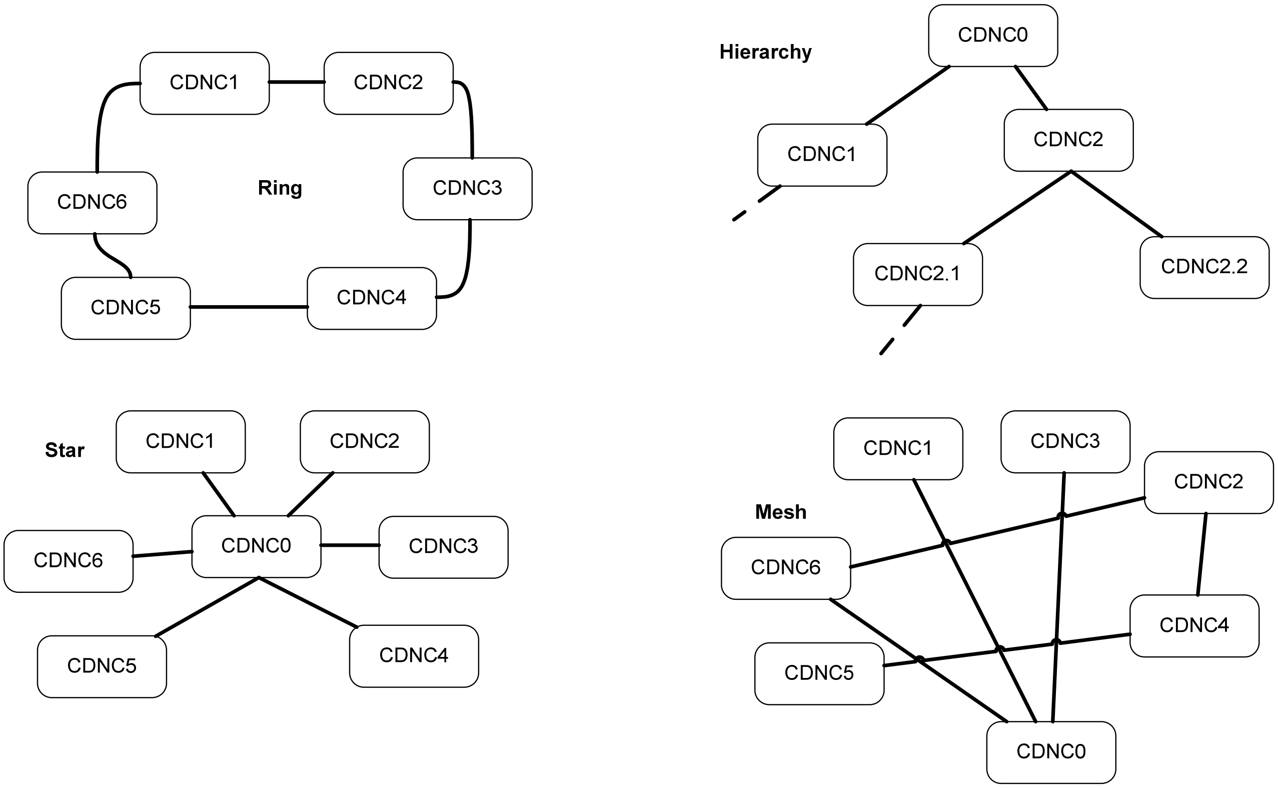


Figure 7.4-1: CDNC organization examples

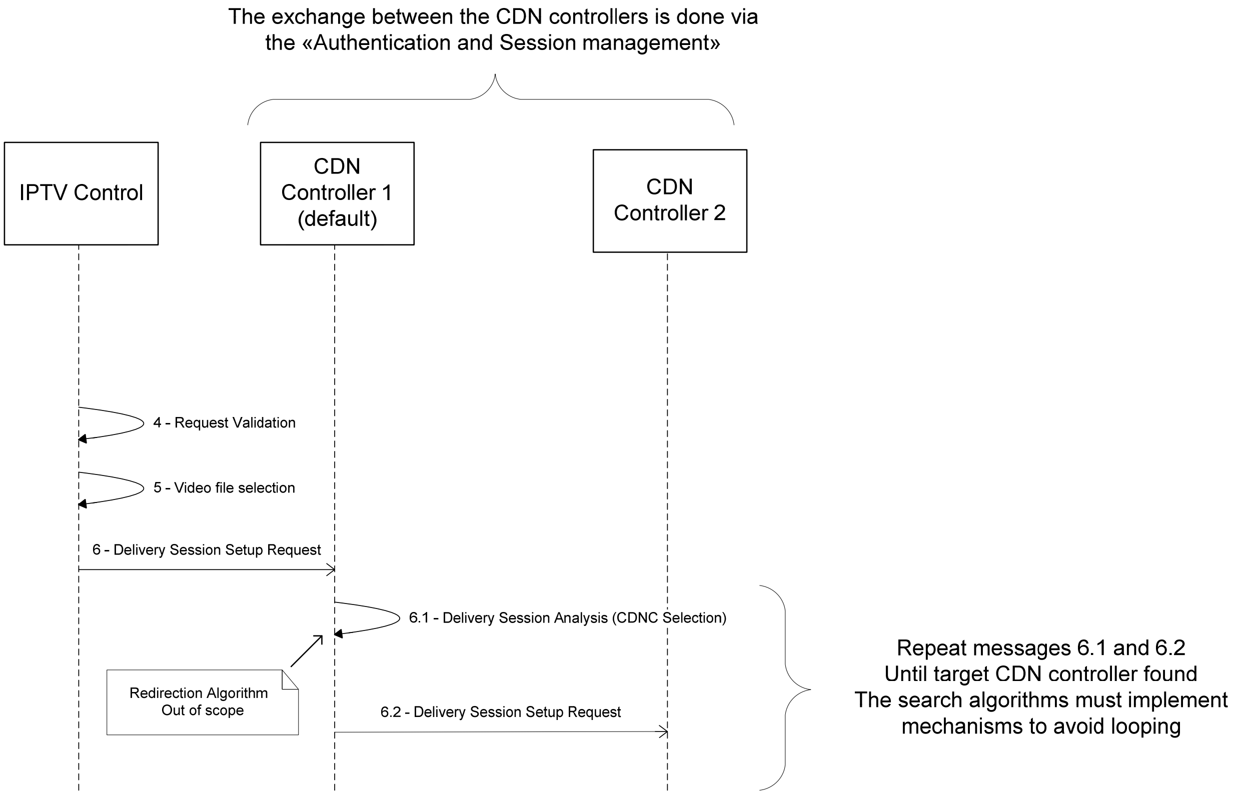

The exchange between the CDN controllers is done via the «Authentication and Session management»
IPTV Control
CDN Controller 1 (default)
CDN Controller 2
4 - Request Validation
5 - Video file selection
6 - Delivery Session Setup Request
6.1 - Delivery Session Analysis (CDNC Selection)
Redirection Algorithm Out of scope
6.2 - Delivery Session Setup Request
Repeat messages 6.1 and 6.2
Until target CDN controller found
The search algorithms must implement
mechanisms to avoid looping

Figure D-2: 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 16]..

The examples and description within this section are based on IMS AKA authentication mechanisms described in section 7.4.2.1. 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[2]network 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[3] 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 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.

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

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

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, 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 1.

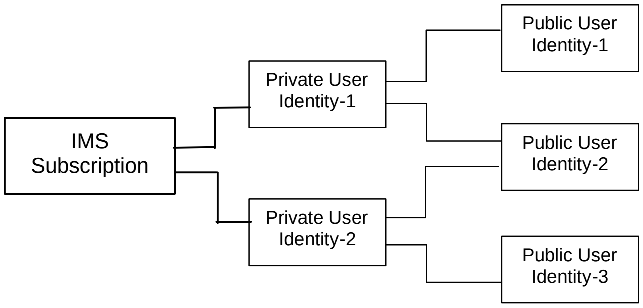


Figure 1: Relationship of the Private User Identity and Public User Identities

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

A IMS Service Profile is a collection of service and user related data as defined in TS 29.228 [Ref 27]. 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 2.

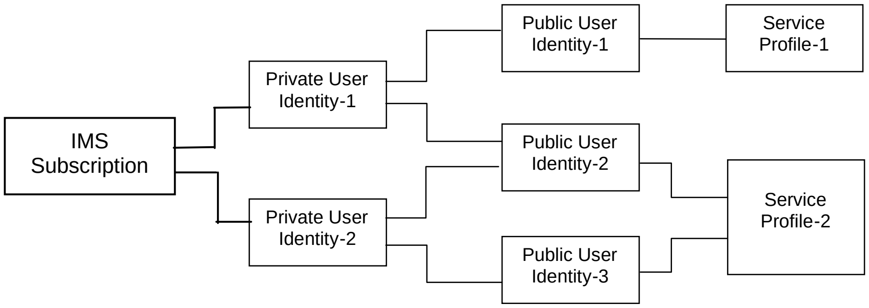


Figure 2: Relationship of the Private User Identity and Public User Identities to Service Profiles

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 16]

Each IMS Public Identity associated with an IMS-IPTV subscription, represents an user within the household. This identity is used when the user “logs on” to the ITF for personalized IPTV services using a 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 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 house.

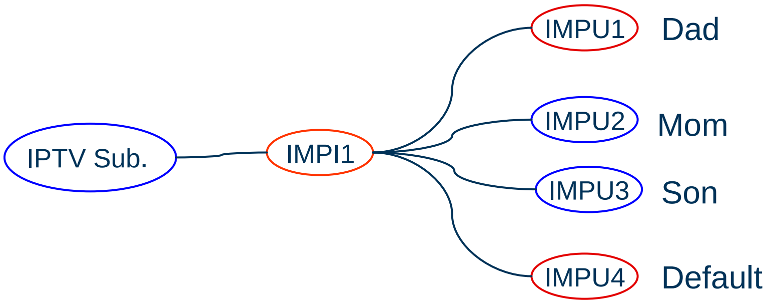


Figure 3: All IMPUs associated with a single IMPI.

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 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.

,

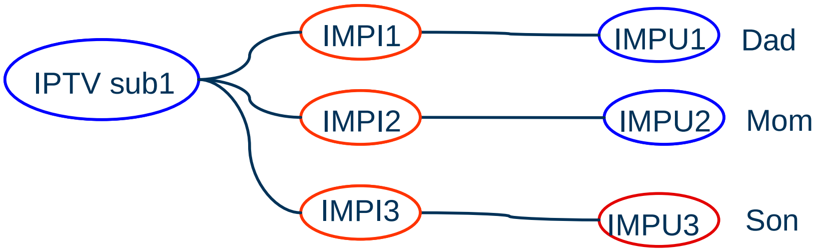


Figure 4: 1:1 IMPU <-> IMPI relationship

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 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

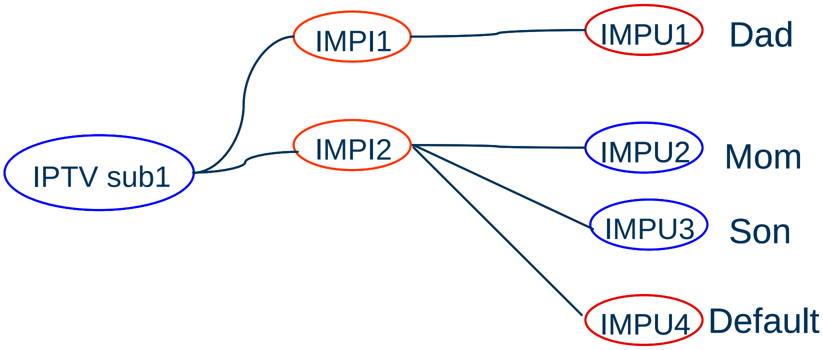


Figure 5: Mixed IMPU <-> IMPI relationships

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.

Option 2 : Multiple UICCs in the household with Single OITF

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.

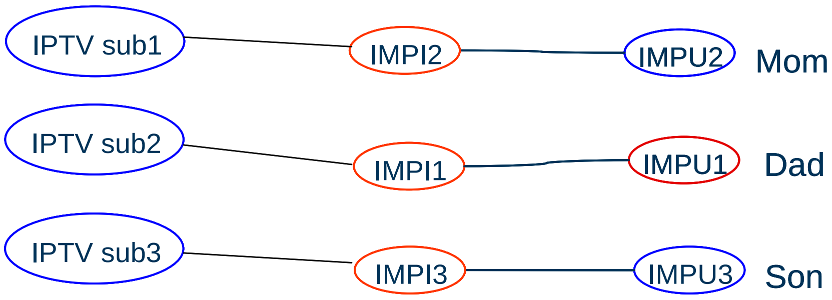


Figure 6: Multiple UICCs

Pros :

- Complete privacy (no potential for any sharing)
- Aligned with todays 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 house hold since

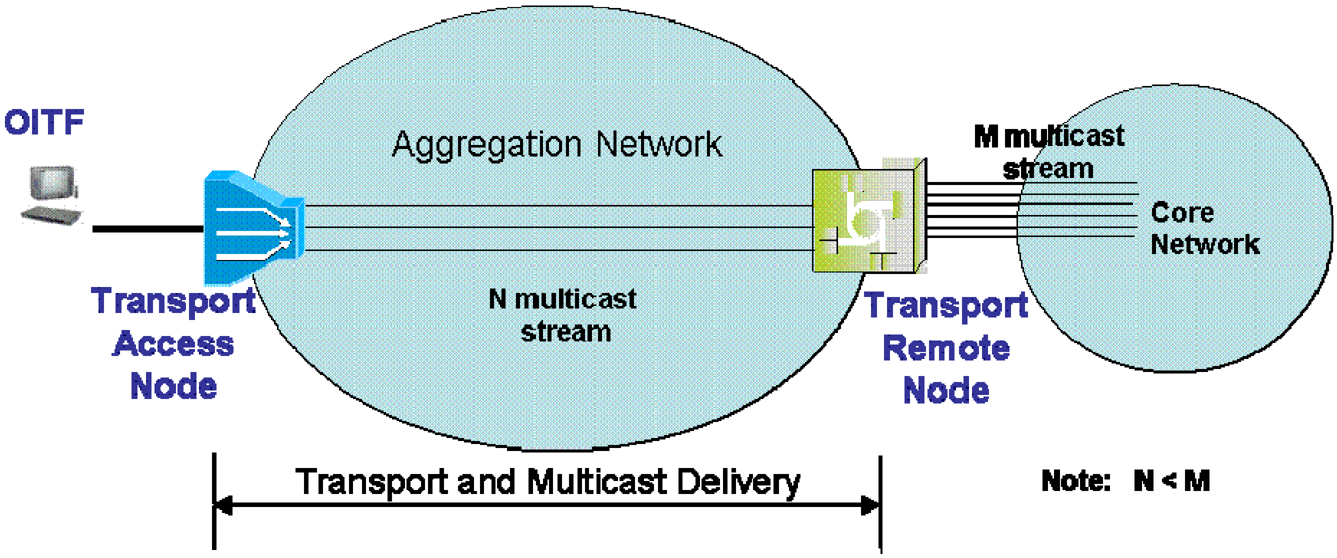
Appendix E. Resource and Admission Control for multicast (informative)

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

The solution described in this Annex is purely functional. All the examples refer to xDSL, but their applicability can easily be extended to other types of other access technologies (e.g. GPON networks),.

E.1 Transport and Multicast Delivery Function description

Operator 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): is the access node
- Transport Remote Node (e.g. IP Edge or Feeder): is the network element that resides at the boundary between core networks and access networks.
- Aggregation: is 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 easily extended to more complex aggregation network configurations.

Note that not every multicast channel is usually present at Transport Access Node (e.g. DSLAM), and the number of multicast stream 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 to see a channel that at the moment is not already present at the Transport Access Node .

In particular, during multicast channel selection, the Transport Access Node terminates or proxies to the Transport Remote Node IGMP messages sent from user (IGMP messages belongs to the Content Delivery Session) and/or sends PIM messages to the Transport Remote Node , depending on whether the Transport Access Node is a layer 2 or 3 device (in the following examples and call flows a layer 3 Transport Access Node is considered, but the examples can easily be extended to other deployments).

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 of the new channel required is not present in the Transport Access Node , in order to guarantee the needed bandwidth to 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 authorized bandwidth in the last mile matches the one needed by 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 bandwidth in the last mile doesn’t match the one needed by channel to be viewed, an interaction between the Transport Access Node and Admission Control entities is needed, to verify that there is enough bandwidth in the Access Network;

[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 matches the one needed by channel to be viewed:

- a PIM or IGMP request is sent by the Transport Access Node to the Transport Remote Node ;
- the Transport Remote Node checks if there is enough bandwidth in the Aggregate Network;
- the Transport Remote Node replicates the multicast stream to the Transport Access Node , which streams the channel to the user;

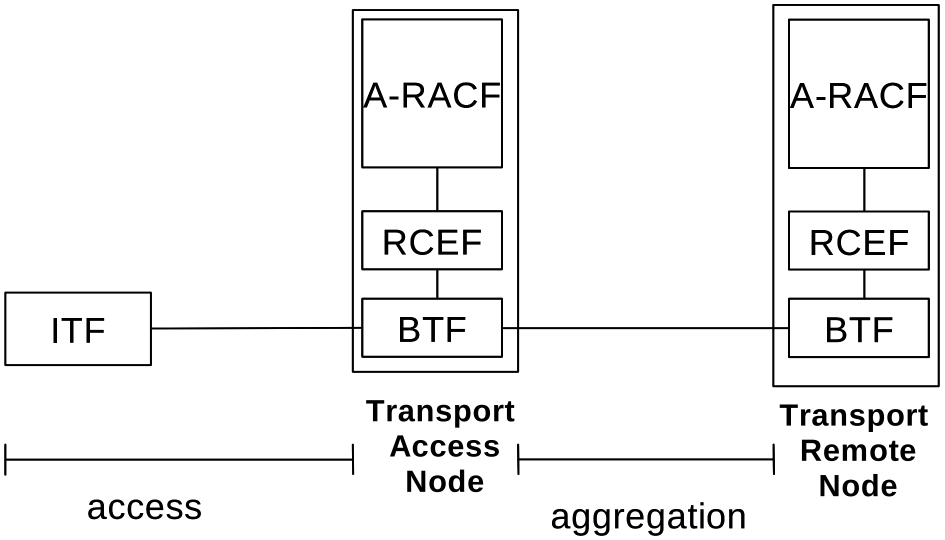
[4] if the stream of the channel requested by the user is not received by the Transport Access Node , and the bandwidth in the last mile does not match the one needed by channel to be viewed:

- the Transport Access Node check that there is enough bandwidth in the Access Network;
- a PIM or IGMP request is sent by the Transport Access Node to the Transport Remote Node ;
- the Transport Remote Node checks that there is enough bandwidth in the Aggregate Network;
- the Transport Remote Node replicates the multicast stream to the Transport Access Node , which streams the channel to the user.

Section 5.2.3 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 he Transport Remote Node performs admission control for the aggregation segment.

The following paragraph details some of the call flow related to the 4 cases considered above.



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 bandwidth in the last mile does not match the one needed by 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 bandwidth in the last mile does not match the one needed by channel to be viewed (case 2 considered in the previous section);

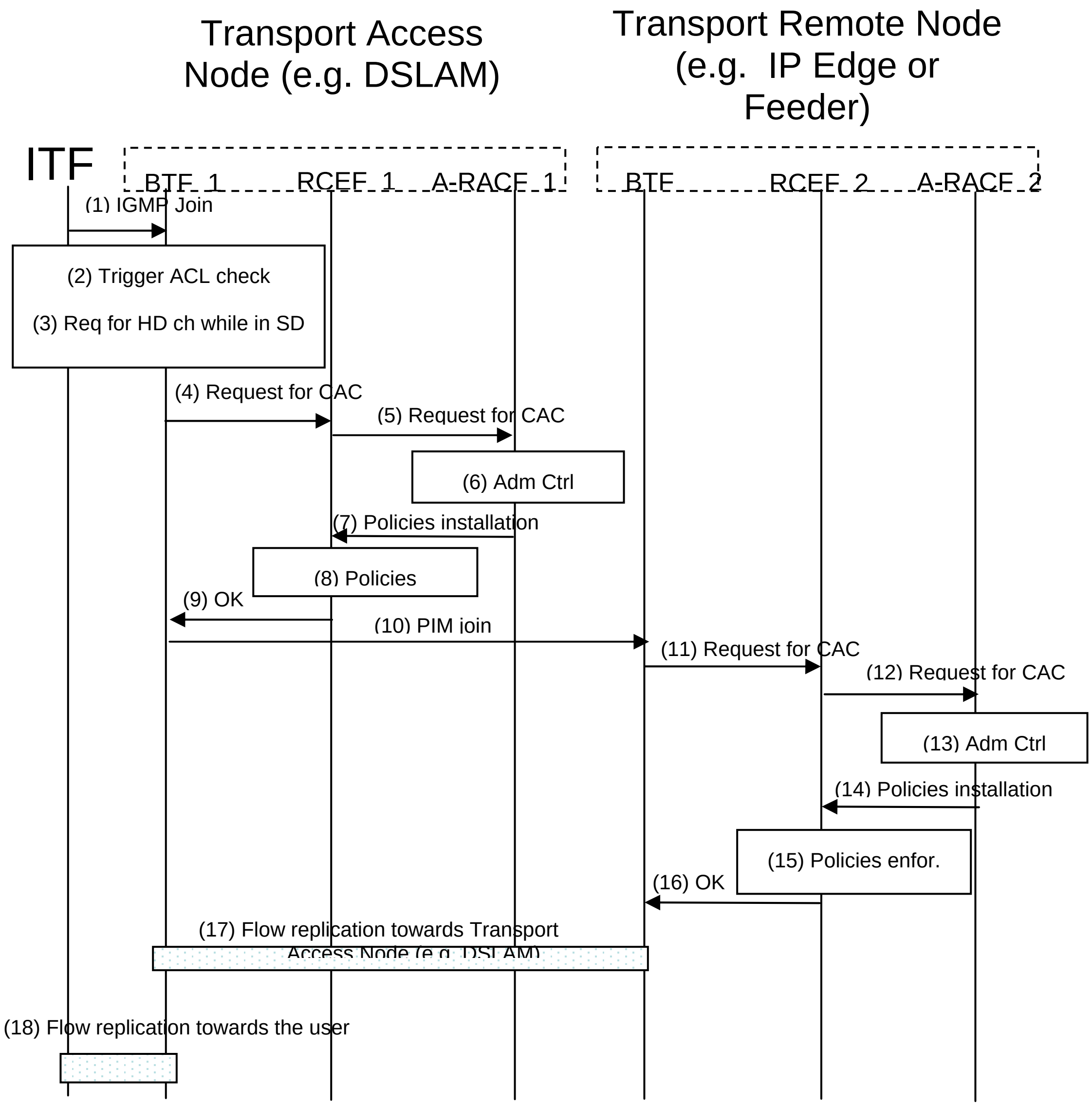
- Access Control List are pre-provisioned in the Transport Access Node to authorize the user request;

- The association between channels (or group of channels) and the bandwidth 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 .

Other deployment configuration 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 bandwidth in the last mile doesn’t match the one needed (case 4)


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) Req for HD ch while in SD
(4) Request for CAC
(5) Request for CAC
(6) Adm Ctrl
(7) Policies installation
(8) Policies
(9) OK
(10) PIM join
(11) Request for CAC
(12) Request for CAC
(13) Adm Ctrl
(14) Policies installation
(15) Policies enfor.
(16) OK
(17) Flow replication towards Transport Access Node (e.g. DSLAM)
(18) Flow replication towards the user

The description of the steps is the following

(1) The ITF requests an HD channel via IGMP Join

(2) The IGMP message triggers in the Transport Access Node the check of the pre-provisioned ACL to authorize the request

(3) Since the requested channel requires more bandwidth than the channel currently accessed, 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 for obtaining 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 CAC towards the RCEF

(12) The RCEF builds an admission control request and sends it to the A-RACF

(13) The A-RACF in the Transport Remote Node performs admission control on the aggregation network and derives the traffic policies to be installed in the RCEF

(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 ECF 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 bandwidth in the last doesn’t mile match the one needed (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 Access Network, and streams the channel to the user.

See figure of Case 4 from step 1) to 9) and step 18).

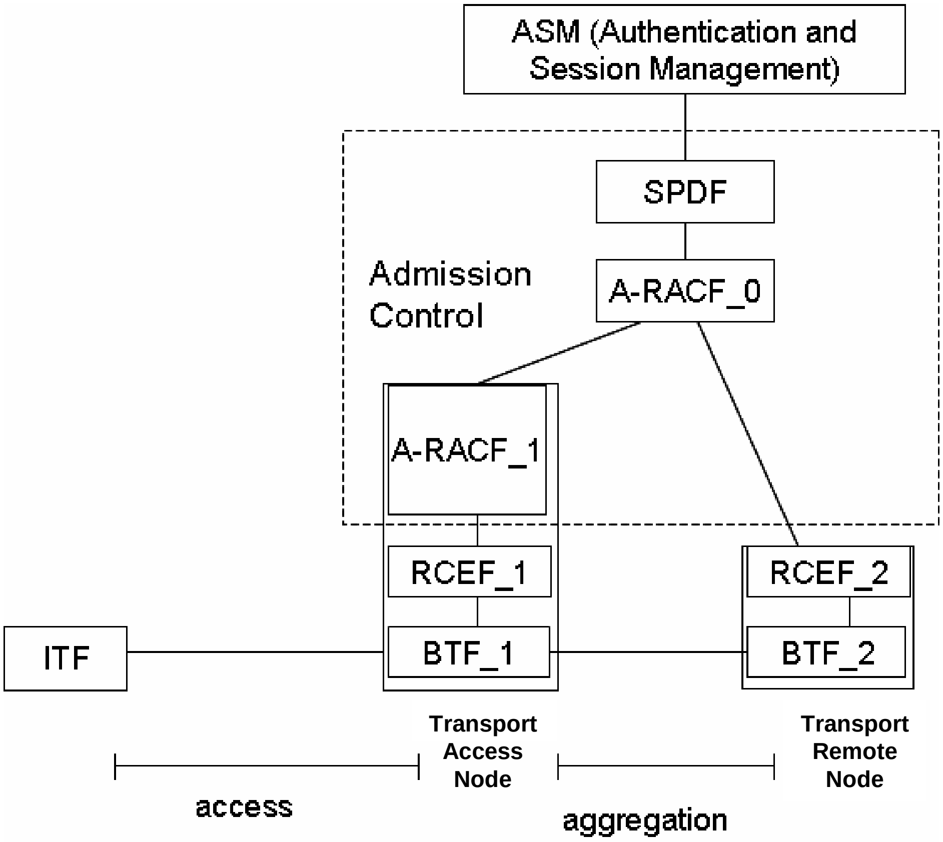
E.3 Linear TV and VoD unified view for reservation on Access segment

In this chapter an example of information flow is provided to illustrate how an unified Linear TV and VoD Admission Control works with the architectural solution described in this Annex.

The examples have the following assumptions:

- Linear TV and VoD service share the same transport resource in the Access segment
- Linear TV and VoD 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 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 Access 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 VoD in the Aggregation Segment and in the Access Segment. It is further handling Admission Control for Linear TV in the Access 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 Access segment.

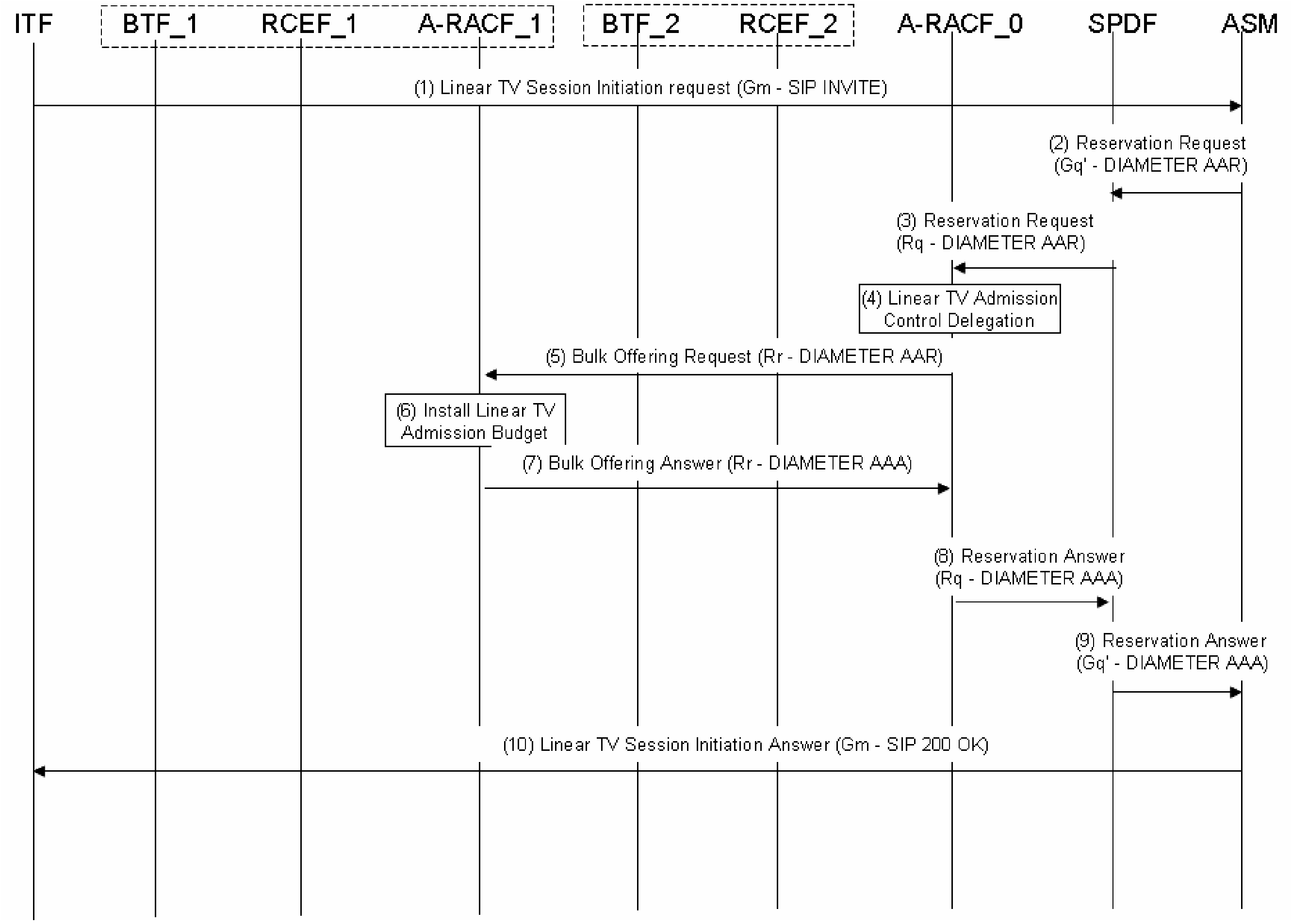


The Information flow for delivering both Linear TV and CoD comprises 3 phases:

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.


ITF
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)

1. The user requests access to Linear TV

2-3. Reservation request

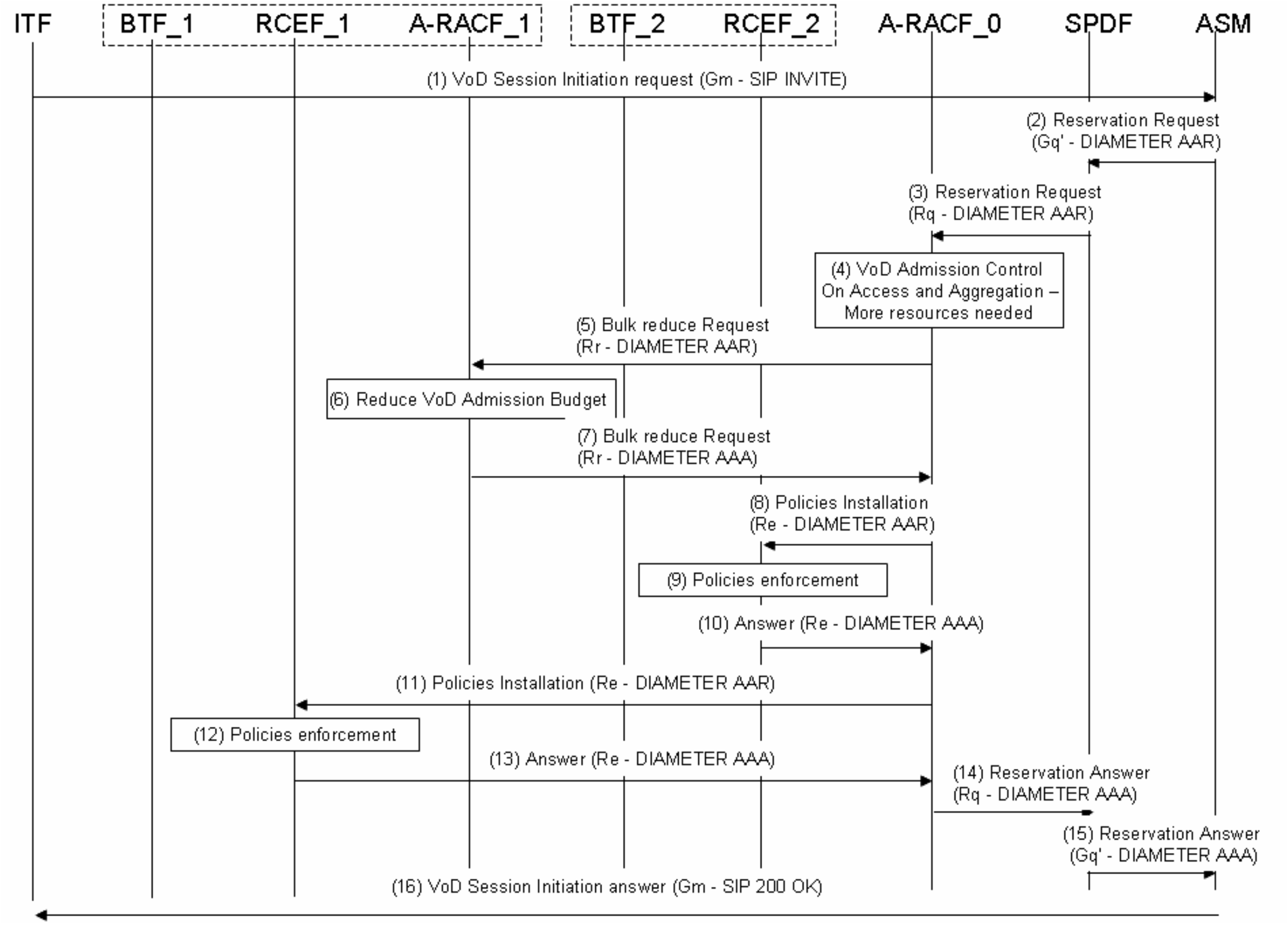
4/7. A-RACF_0 installs a bandwidth budget in A-RACF_1

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 has not sufficient resources to fulfil the request in the access segment. Then it asks the needed resources to A-RACF_1 by reducing its Linear TV budget.


ITF
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 Request (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)

1. The user requests access to CoD

2-3. Reservation Request

4/7. A-RACF_0 requests the needed bandwidth to A-RACF_1. These cannot be mandatory. This must be policy based.

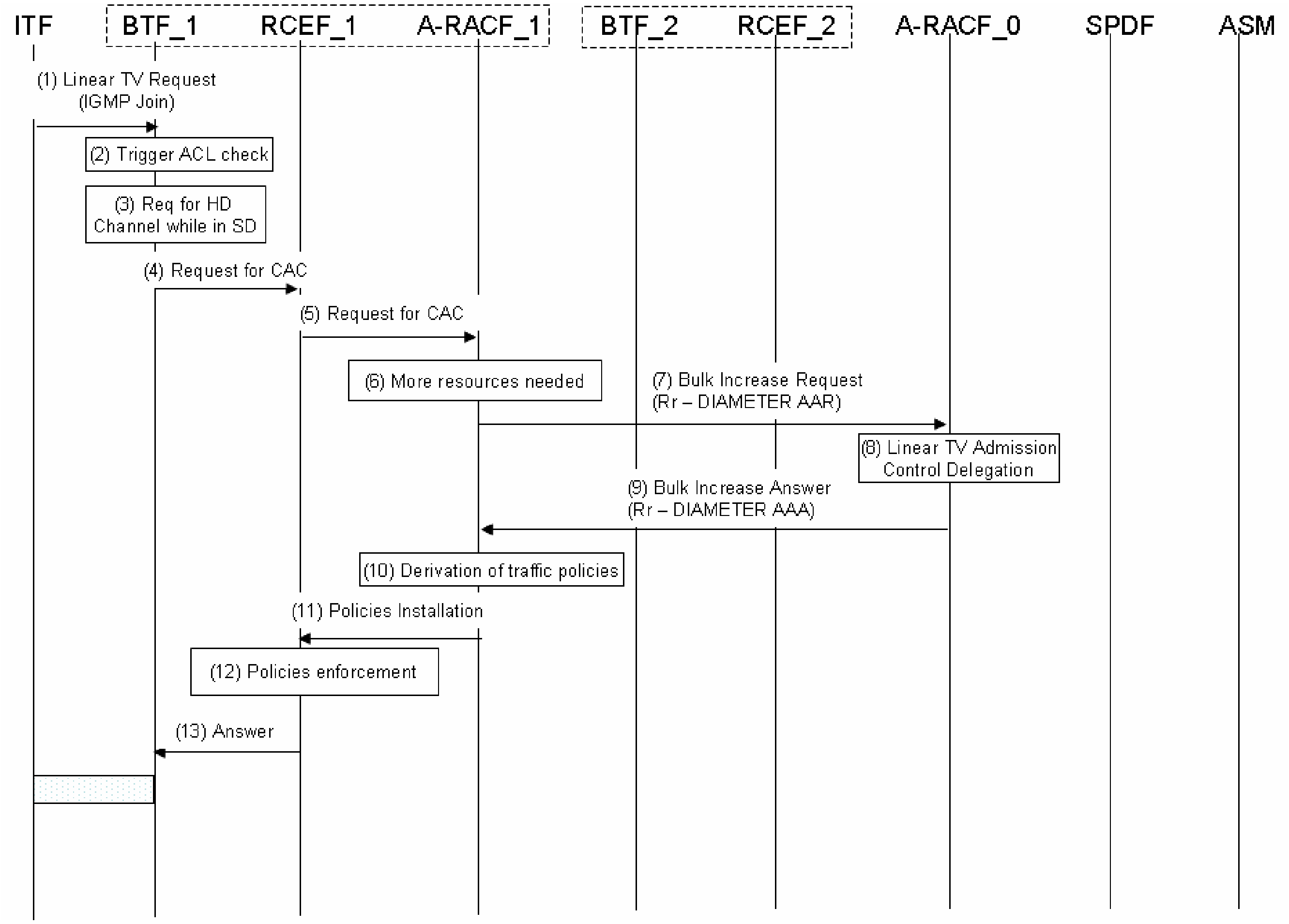
8/13. Policies installation in the RCEFs

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.


ITF
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) Req 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

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. Policies installation. What are these policies enforcing?

13. Answer and Linear TV flow delivery

E.4 Applicability to other access technologies

The solution described in this document is purely functional. All the examples in the chapter above refer to xDSL, but its applicability can easily be extended to other types of other access technologies.

For example in GPON networks, the BTF-RCEF-A-RACF for supporting Linear TV may be deployed in the OLT, keeping the same level of functionalities as described above.

Appendix F. Change History (Informative)

Date	Version	Change
2007-09-18	V1.0 2007-09-18 Editor’s Copy	Clean output from the Seoul Meeting with only editorial changes added + removal NPI-13 (see George Foti’s email) and addition of Annex E (which was mistakenly not added in Seoul).