ETSI TR 102 469 V1.1.1 (2006-05)

Technical Report

Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Architecture

Reference
DTR/JTC-DVB-185

Keywords
broadcasting, data, digital, DVB, IP, video

ETSI

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

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

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

Contents

Intellectual Property Rights

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

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

Foreword

This Technical Report (TR) has been produced by Joint Technical Committee (JTC) Broadcast of the European Broadcasting Union (EBU), Comité Européen de Normalisation ELECtrotechnique (CENELEC) and the European Telecommunications Standards Institute (ETSI).

NOTE: The EBU/ETSI JTC Broadcast was established in 1990 to co-ordinate the drafting of standards in the specific field of broadcasting and related fields. Since 1995 the JTC Broadcast became a tripartite body by including in the Memorandum of Understanding also CENELEC, which is responsible for the standardization of radio and television receivers. The EBU is a professional association of broadcasting organizations whose work includes the co-ordination of its members' activities in the technical, legal, programme-making and programme-exchange domains. The EBU has active members in about 60 countries in the European broadcasting area; its headquarters is in Geneva.

European Broadcasting Union
CH-1218 GRAND SACONNEX (Geneva)
Switzerland
Tel: +41 22 717 21 11
Fax: +41 22 717 24 81

Founded in September 1993, the DVB Project is a market-led consortium of public and private sector organizations in the television industry. Its aim is to establish the framework for the introduction of MPEG-2 based digital television services. Now comprising over 200 organizations from more than 25 countries around the world, DVB fosters market-led systems, which meet the real needs, and economic circumstances, of the consumer electronics and the broadcast industry.

Introduction

IP Datacast over DVB-H is an end-to-end broadcast system for delivery of any types of digital content and services using IP-based mechanisms optimized for devices with limitations on computational resources and battery. An inherent part of the IPDC system is that it comprises of a unidirectional DVB broadcast path that may be combined with a bi-directional mobile/cellular interactivity path. IPDC is thus a platform that can be used for enabling the convergence of services from broadcast/media and telecommunications domains (e.g. mobile / cellular).

1 Scope

The present document defines the reference architecture for services delivered by IP Datacast [7] over DVB-H [1]. The reference architecture is provided to illustrate the way the components in IP Datacast over DVB-H work together.

2 References

For the purposes of this Technical Report (TR) the following references apply:

[1] ETSI EN 302 304: "Digital Video Broadcasting (DVB); Transmission System for Handheld Terminals (DVB-H)".

[2] ETSI TR 101 516: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms (GSM 01.04)".

NOTE: http://www.3gpp.org

[3] ITU-T Recommendation I.112: "Vocabulary of terms for ISDNs".

NOTE: http://www.itu.org

[4] IETF RFC 1208: "A Glossary of Network Terms".

[5] ETSI EN 300 468: "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems".

[6] ETSI EN 301 192: "Digital Video Broadcasting (DVB); DVB specification for data broadcasting".

[7] ETSI TS 102 468: "Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Set of Specifications for Phase 1".

[8] ETSI TR 102 473: "Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Use Cases and Services".

[9] ETSI TS 102 471: "Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Electronic Service Guide (ESG)".

[10] ETSI TS 102 472: "Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Content Delivery Protocols".

[11] ETSI TS 102 470: "Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Program Specific Information (PSI)/Service Information (SI)".

[12] ETSI TS 102 474: "Digital Video Broadcasting (DVB); IP Datacast over DVB-H: Service Purchase and Protection".

[13] ETSI TS 102 005: "Digital Video Broadcasting (DVB); Specification for the use of Video and Audio Coding in DVB services delivered directly over IP protocols".

[14] IETF RFC 2326: "Real Time Streaming Protocol (RTSP)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions given in [2], [3], [11] and the following apply:

bearer: information transmission path of defined capacity, delay and bit error rate, etc.

bearer network: network used to carry the messages of a transport-layer protocol between physical devices

broadcast: unidirectional distribution to all receivers

delivery system: physical medium by which one or more multiplexes are transmitted

NOTE: E.g. satellite system, wideband coaxial cable, fibre optics, terrestrial channel of one emitting point [11].

DVB network: collection of MPEG-2 Transport Streams, each carrying a multiplex, and transmitted on a single delivery system

NOTE: DVB network is identified by network_id, TS 102 470 [11].

ESG fragment: fragment of ESG data delivered in the ESG stream and referred to by a fragment reference in the encapsulation structure

NOTE: Namely an ESG Fragment can be according to TS 102 471 [9] an ESG XML Fragment, ESG Auxiliary Data or Private Auxiliary data.

ESG fragment container: a structure to group one or more ESG Fragments into one data object for transport purposes

interface: common boundary between two associated systems (source: TR 101 516 [2], ITU-T Recommendation I.112 [3]).

IP datacast baseline: the minimum core protocol profile an IPDC DVB-T/H Receiver may expect to be available on IPDC DVB-T/H Bearer (data transmission baseband) and the IPDC DVB-T/H Network is expected to make available on the IPDC DVB-T/H Bearer, TS 102 470 [11]

IPDC DVB-T/H bearer: link and physical layers into which IP platform is encapsulated [11]

IPDC DVB-T/H receiver: equipment or system that acquires IP Datacast based services provided over the IP Datacast Baseline on DVB-H [11]

IPDC DVB-T/H terminal: equipment that constitutes a collection of one or more endpoints for IP Datacast services and that has implemented the full (broadcast) downstream end functionality for one or more IP Datacast services

NOTE: It includes an *IPDC DVB-T/H receiver*. It may include an interaction channel.

IP flow: stream of IP datagrams each sharing the same IP source and destination address

NOTE: An IP flow is identified within an IP platform by its source and destination addresses. IP flows on different IP platforms may have the same source/destination addresses, but are considered different IP flows. IP flow may be delivered over one or more IP streams.

IP platform: set of IP flows managed by an organization

NOTE: The IP platform represents a harmonized IP address space that has no address collisions. An IP platform may span several Transport Streams within one or more DVB networks. Several IP platforms may co-exist in the same Transport Stream. IP platform is identified by platform_id, TS 102 470 [11].

IP stream: data stream delivering exactly one MPE encoded IP datagram stream

NOTE: IP stream is identified by transport_stream_id, original_network_id, service_id, component_tag and IP source/destination addresses, TS 102 470 [11].

protocol: formal set of procedures that are adopted to ensure communication between two or more functions within the same layer of a hierarchy of functions, (source: ITU-T Recommendation I.112 [3])

Reference point: conceptual point at the conjunction of two non-overlapping functional groups

NOTE: It consists of none or any number of interfaces of any kind, (source: ITU-T Recommendation I.112 [3]).

Service Access Point (SAP): point at which the services of an OSI layer are made available to the next higher layer

NOTE: The SAP is named according to the layer providing the services: e.g. Transport services are provided at a Transport SAP (TSAP) at the top of the Transport Layer, RFC 1208 [4].

Interface, Reference Point and *Protocol* differentiated at a glance:

- A *reference point* is just a label between two groups of logical entities in the overall architecture.
- Function level architecture (like the one for ESG in the present document) takes a step to details and maps functional elements of a given function to the overall architecture.
- The relation between two functional entities is called *interface* and shall be specified. One or more *protocols* may be part of the specification.

3.2 Abbreviations

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

ALC	Asynchronous Layered Coding
BAT	Bouquet Association Table
CBMS	Convergence of Broadcast and Mobile Services
DVB	Digital Video Broadcasting
DVB-H	DVB-Handheld
ECM	Entitlement Control Message
EDGE	Enhanced Data rates for Global Evolution
EMM	Entitlement Management Message
ESG	Electronic Service Guide
ESGC	ESG Container
FEC	Forward Error Correction
FFS	For Further Study
FLUTE	File DeLivery over Unidirectional Transport
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile Communication
HTTP	HyperText Transfer Protocol
INT	IP/MAC Notification Table
IP	Internet Protocol
IPDC	IP DataCast
ISO	International Standards Organisation
KMM	Key Management Message
KMS	Key Management System
KMSA	Key Management System Agent
KSM	Key Stream Message
LCT	Layered Coding Transport
MMS	Multimedia Message Service
MPE	Multi-Protocol Encapsulation
NIT	Network Information Table
OMA	Open Mobile Association
OSI	Open Systems Interconnection
PAT	Program Association Table
PEK	Programme Encryption Key
PMT	Program Map Table
PSI	Program Specific Information
RO	Rights Object
RTP	Real-Time Protocol
RTSP	Real Time Streaming Protocol
SAP	Service Access Point
SDP	Session Description Protocol
SEK	Service Encryption Key
SI	Service Information
SMS	Short Message Service
TCP	Transmission Control Protocol
TEK	Traffic Encryption Key
TS	Transport Stream
UDP	User Datagram Protocol

UMTS	Universal Mobile Telecommunication System
WAP	Wireless Application Protocol
XML	eXtended Markup Language

4 Functional Architecture

The functional architecture is a general technical framework for the system to be specified. It describes the current best understanding of the basic functional elements of the system with an assignment to key system functionalities.

The architecture is intended to leave room for technical implementation alternatives. The links between the elements illustrate the possible exchange of information, operational parameters, delivered services, etc.

4.1 Architectural Model

IP Datacast over DVB-H involves a number of functional entities over a set of reference points. Figure 1 shows the functional entities and their relationships. The following clauses provide additional information on functional entities and reference points.

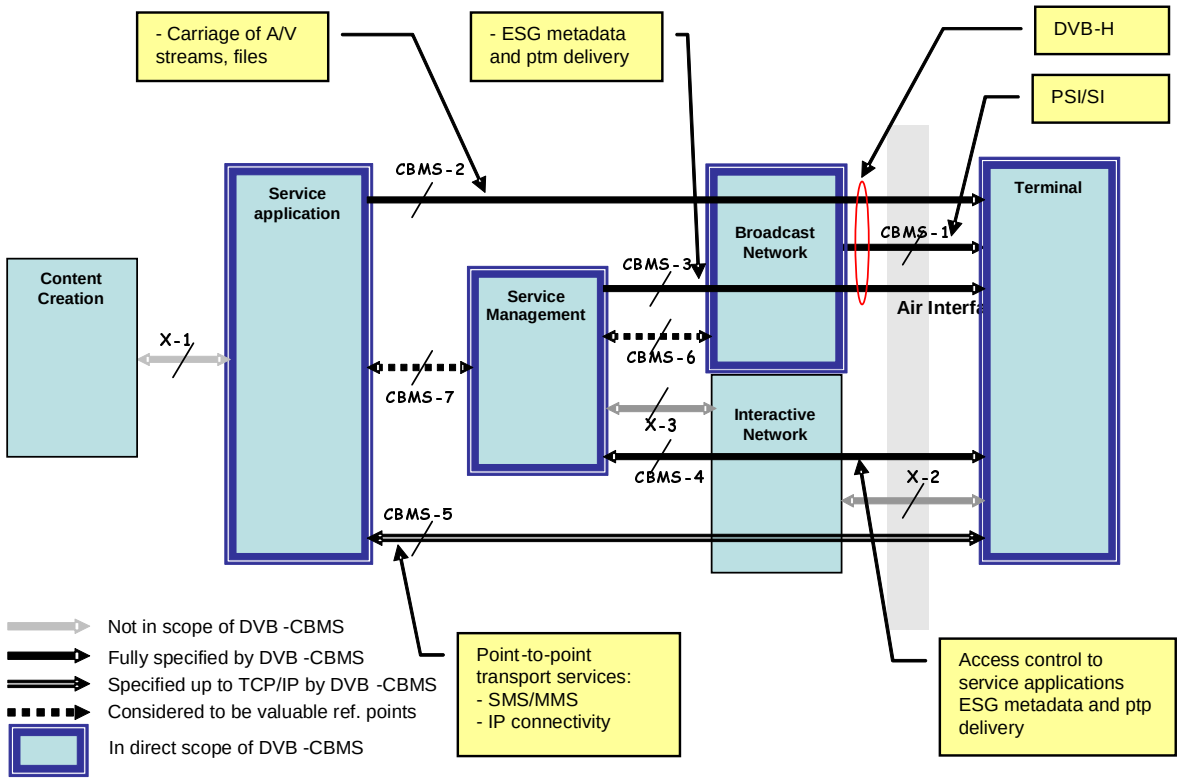

Figure 1: Proposed Architecture Diagram

4.2 Functional Entities

IP Datacast over DVB-H involves a collection of entities that work together in order to achieve the required capabilities. The following table presents these functional entities. The table includes functional entities that provide services described within the scope of DVB-CBMS and other functional entities that provide services but which are defined elsewhere.

Table 1: Description of functional entities

Functional Entity Name	Description
Entities in the scope of DVB-CBMS specification	
Service Application	Aggregates content from multiple sources and their related metadata in order to provide a particular service application. Provides the head-end application logic. Responsible to provide content encoded in the format understood by the terminal either via streaming or file carousel delivery. Generates service description metadata to be used in the Electronic Service Guide (to be provided at CBMS-7). Interaction end-point for terminals to interact with service application. Service Protection provision. A Service Application entity may exist for each application that is provided in IP Datacast.
Service Management	Consists of four sub-entities, which may be instantiated independently: 1. Service configuration and resource allocation: • Registration of service applications that contend for bandwidth of the broadcast bearer (i.e. one DVB-H IP platform in one DVB transport stream). • Assignment of services to location (wrt. Broadcast network topology), to bandwidth and schedules services over time. • There is one instance of this sub-entity associated with a broadcast bandwidth contention domain. 2. Service Guide Provisioning application: • Aggregation of ESG (metadata information) pieces from the service applications. • There may be multiple instances of this sub-entity. 3. Security/service protection provision: • Management of user access to service applications. 4. Location services: • The service management entity may provide location services to service application(s) in a manner that is independent of the way they are actually obtained (such as interaction bearer network functionality or GPS).
Broadcast Network	Multiplexing of service applications at IP level. Assignment of IP flows on DVB-H time slices (IP Encapsulation). Transmission over DVB-H. Security/service protection provisioning TBD.
Terminal	The user device. Point of acquisition and consumption for content. Client of network and service resources.
Entities out-of-scope of DVB-CBMS specification	
Content Creation	This is the primary source of content for distribution over IP Datacast. It may provide support for delivery paradigms, such as streaming. Provides base material for content descriptions.
Interactive Network	Provision for terminal to interact with service management and/or service application. This entity exists only if the IPDC terminal includes an endpoint for it and if service management and/or service application support the relevant reference points. Service applications may require communication over the interactive network. May provide additional functionalities to Service Application or Service Management, such as Location Services (may require additional reference point) Security/service protection provisioning TBD.

4.3 Reference Points

The functional entities defined in the IP Datacast over DVB-H architecture are connected to allow them to provide the services required. These connection points establish the reference points documented in this clause. As with functional entities, certain of these reference points will be fully defined as part of the IP Datacast over DVB-H standard.

Table 2: Description of reference points

Reference Point Name	End Points	Usage
Reference point in the scope of the IP Datacast over DVB-H specification		
CBMS-1	*From* Broadcast network *To* Terminal	Broadcast network-specific singnalling, PSI/SI signalling in DVB-H.
CBMS-2	*From* Service Application *To* Terminal	Content flow, including: • A/V streams. • Auxiliary data. • Files delivered by a carousel mechanism (clips, software, etc.).
CBMS-3	*From* Service Management *To* Terminal	Electronic Service Guide (metadata, point-to-multipoint delivery).
CBMS-4	*Between* Service Management *And* Terminal	Access control to service applications. Electronic Service Guide (metadata, point-to-point delivery). This reference point exists only if the IPDC terminal includes an endpoint for the interactive network and if service management supports this reference point.
CBMS-5	*Between* Service Application *And* Terminal	Point-to-point transport services (SMS/MMS, IP connectivity). This reference point exists only if the IPDC terminal includes an endpoint for the interactive network and if service application supports this reference point. Service applications may require this reference point.
Reference Points considered valuable for the IP Datacast over DVB-H architecture, but are not covered by the baseline specification for reference points spanning the air interface.		
CBMS-6	*From* Service Management *To* Broadcast Network	Configuration of the DVB-H transport (number of services, allocated bandwidth, etc.).
CBMS-7	*Between* Service Application *And* Service Management	Service application declaration. Service application description, including content description/metadata.
Reference Points out-of-scope of IP Datacast over DVB-H specification		
X-1	*Between* Content Creation *And* Service Application	Provision of content to Service Application, including: • Content essence. • Content description/metadata. • Content control policy, (see note).
X-2	*Between* Interactive Network *And* Terminal	Interactive network specific interactions (authentication, mobility management, specific services such as voice, etc.).
X-3	*Between* Service Management *And* Interactive Network	This reference point may be used to access specific functions available in the interactive network, such as subscriber management or billing functions.
NOTE: Although out-of-scope of DVB-CBMS specification, the DVB forum has specified standards that may be used for this reference point.		

4.4 Air Interface

The functional entities in the IP Datacast over DVB-H architecture are arranged such that a collection of *head-end* entities provide services to the terminal entity (i.e. wireless user terminals). All entities found in the architecture but the terminal entity are head-end entities.

The Air Interface is constituted by the union of all reference points between any of the head-end entities and the terminal entity.

5 End-to-end operations

The following clauses describe how the reference architecture is applied to the different aspects of end-to-end operations defined in IP Datacast. In particular, the logical entities are detailed and logical sub-entities are identified, which are involved in one or more end-to-end operation aspects.

5.1 Service configuration

Service configuration concerns both, configuring the service in the head-end and configuring reception of service(s) in the terminal. Configuration in the head-end is a prerequisite for the terminal in order to be able to configure for the service reception. This clause shows service configuration on both ends in conjunction.

5.1.1 Logical Entities and Reference Points

Figure 2 identifies sub-entities of the main entities introduced in clause 4 that are involved for the service configuration operation. It also highlights the reference points that are involved in this operation.

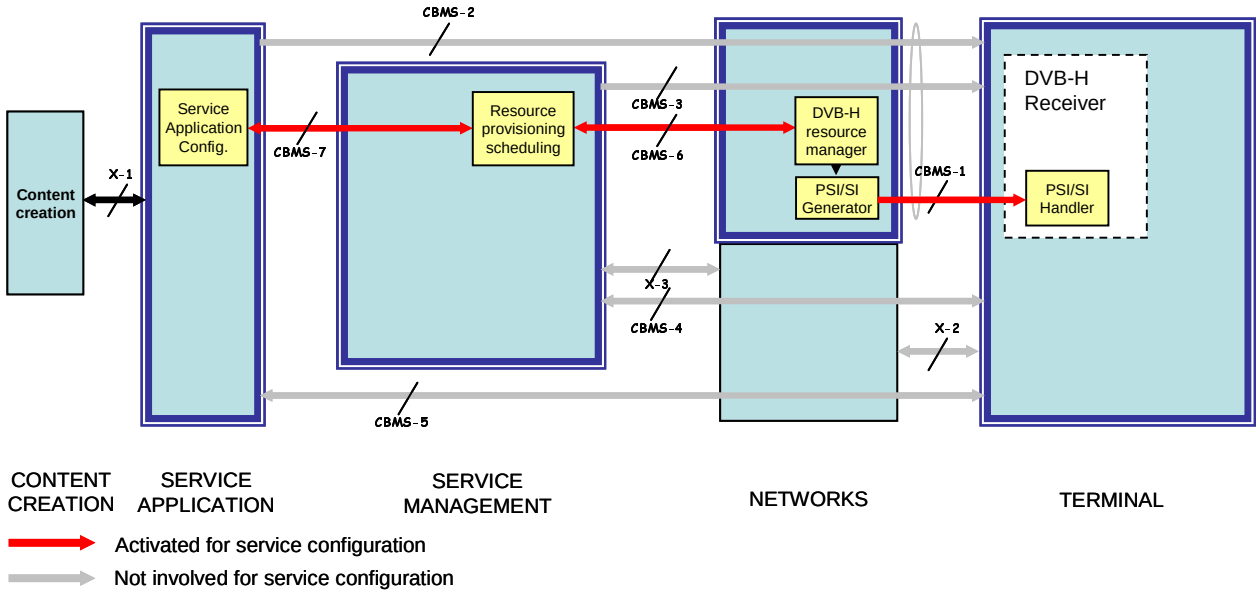

Figure 2: Reference points activated for service configuration

Table 3 describes the sub-entities introduced in figure 2.

Table 3: Description of logical sub-entities involved in service configuration

Logical sub-entity	Logical Entity it is part of	Involved Ref. Points	Description
Service application configuration	Service Application	CBMS-7	Entity requesting transmission resources (e.g. bandwidth, source/ destination IP addresses, port numbers, protocols, scheduling, etc.) from Service Management Gathered information is recorded for configuration of service delivery and ESG acquisition information.
Resource provisioning and scheduling	Service Management	CBMS-7, CBMS-6	Entity translating the logical service requests into physical resource requests (e.g. bit rate, burst cycle time, MPE-FEC, etc.). Typical services are audio streams, A/V streams, ESG, etc. It is assumed that each service management entity logically contains one instance of this sub-entity per DVB-H resource manager it is connected to.
DVB-H resource manager	Broadcast Network	CBMS-6	Part of the head-end that handles the resource requests and configures the transmission equipment (typically includes IP encapsulator and DVB multiplexer). It is assumed that at the logical level one DVB-H resource manager instance manages one IP platform.
PSI/SI Generator	Broadcast Network	CBMS-1	Entity generating DVB-H specific tables or descriptors (in particular NIT, (BAT), PAT, PMT, INT). It may be part of an IP encapsulator.
PSI/SI Handler	Terminal	CBMS-1	Part of the DVB-H receiver in the terminal entity to extract and interpret DVB-H relevant PSI/SI information.

5.1.2 Message Flow

Figure 3 shows the logical flow of messages between the entities/sub-entities involved. Some of the messages exchanged for service configuration in the head-end may not be exchanged automatically, but in some other informal way.

The Message Sequence assumes the following precondition:

- A service level agreement is in place between the Service Application operator and Service Management operator and also between Service Management and Broadcast Network.

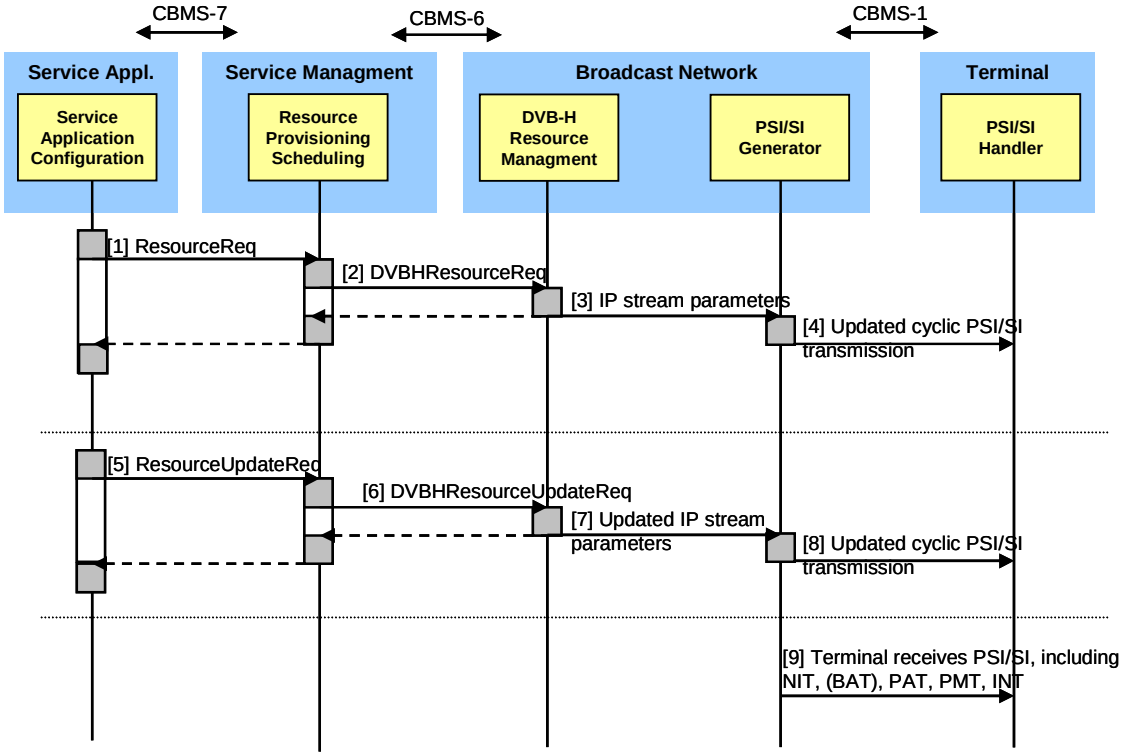

Figure 3: Message flow for service configuration

Table 4 describes the messages shown in figure 3 in detail.

Table 4: Description of logical messages for Service Configuration

1	**ResourceReq** The request performs the initial registration of a service with the service management and allows it to request an initial set of resources. The request needs to be authenticated by the Service Management. Service applications issues this request with specifications for bandwidth, scheduling, source/destination IP addresses, protocol translation, etc. The response includes actual parameters and resources that have been allocated for the service application.
2	**DVBHResourceReq** In response to a ResourceReq. Resource Provisioning/Scheduling issues this request to the DVB-H resource management. It contains an appropriate translation of the resources requested by the service application. The response includes actual parameters and resources that have been allocated, which are then translated into the response message for message 1. There may be instances where this request is issued independently of message 1, e.g. to pre-allocate a resource bundle.
3	**IP stream parameters** The DVB-H Resource Management notifies the IP-to-section mapping sub-entity (part of an IP Encapsulator) of relevant IP parameters, including IP numbers, PID/time-slice assignment, bandwidth, etc.
4	**Updated cyclic PSI/SI transmission** As a result of updated IP stream parameters, the PSI/SI Generator creates updated PSI/SI tables and transmits them repeatedly to terminals.
5	**ResourceUpdateReq** At any time after a service application initially has been configured and registered, it may wish to modify its resource requirements. It issues a ResourceUpdateReq with the updated resource requirements. The response message includes actual parameters and resources that have been updated.
6	**DVBHResourceUpdateReq** In response to a ResourceUpdateReq. Resource Provisioning/Scheduling issues this request to the DVB-H resource management. It contains an appropriate translation of the updated resources requested by the service application. The response includes actual parameters and resources that have been updated, which are then translated into the response message for message 5.
7	**Updated IP stream parameters** See message 3.

8	**Updated cyclic PSI/SI transmission** See message 4.
9	**Terminal receives PSI/SI, including NIT, (BAT), PAT, PMT, INT** In order to configure the terminal for any IP service received over DVB-H, including Bootstrap and specific ESG, the terminal needs to receive and interpret Network Information Table (NIT), Bouquet Association Table (BAT) (if signalled by NIT), Program Association Table (PAT), Program Map Table (PMT), IP/MAC Notification Table (INT), as specified in messages 1, 5 and 6. The terminal retrieves Multicast IP addresses from ESG Acquisition Information (see clause 5.2).

5.2 Electronic Service Guide

The Service Guide function provides the IP Datacast users with information on the various IP Datacast services available in their region. Figure 4 illustrates which of the functional entities and reference points are involved in management and delivery of Electronic Service Guide. Designators of reference points are the same as defined in clauses 4.2 and 4.3.

The end-to-end operation of the ESG includes delivery of ESG data over the broadcast network, or, if available, over the interaction network in push or pull mode. ESG delivery over the interactive network will be added to the specification at a later time.

ESG consists of two essential types of information: user attraction information and acquisition information. The majority of the ESG information is expressed as XML fragments. However, part of the acquisition information are SDP files that the terminal needs to locate service streams and configure service consumption applications appropriately. Other formats of information exist, such as PNG files for logos and pictures.

5.2.1 Logical Entities and Reference Points

Figure 4 identifies sub-entities of the main entities introduced in clause 4 that are involved for the ESG operation. It also highlights the reference points that are involved in this operation.

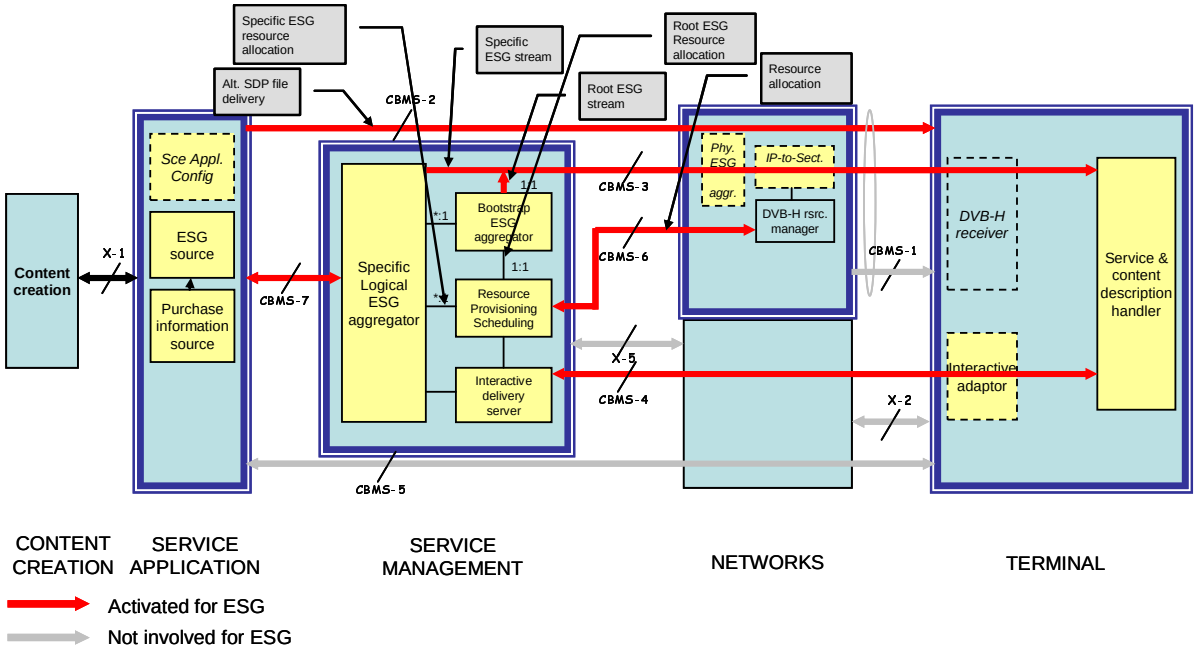

Figure 4: Reference points activated for ESG

Table 5 describes the sub-entities introduced in figure 4.

Table 5: Description of logical sub-entities involved in ESG

Logical sub-entity	Logical Entity it is part of	Involved Ref. Points	Description
ESG Source	Service Application	CBMS-7, CBMS-2	Service application specific source of ESG fragments, comprising attraction information, acquisition information (coming from Service application configuration sub-entity) and purchase information. SDP files, which are part of acquisition information, may be delivered separately from the ESG. In that case the service application may deliver the SDP files over the CBMS-2 reference point.
ESG purchase information	Service Application	Internal to SA	Source of purchasing information contributed to the ESG. Service application may rely on other sources for obtaining this information.
Specific logical ESG aggregator	Service Management	CBMS-7, CBMS-3	Entity receiving ESG information blocks from one or more service applications, aggregating them into one ESG (as perceived by the end user), and generating consistent set of ESG information blocks, including containers; information blocks are output to physical ESG aggregator. ESG logical aggregator is responsible for managing container versions. A service application may contribute to more than one Logical ESG aggregator.
Bootstrap ESG aggregator	Service management	CBMS-3	Entity receiving the ESG announcement information from all specific aggregators and generating the bootstrap ESG stream.
Resource provisioning and scheduling	Service Management	CBMS-6	*Used here for specific configuration of ESG delivery.*
Interactive delivery server	Service Management	CBMS-4	Provides point-to-point access (pull or push) to ESG through interactive network.
Physical ESG aggregator	Broadcast Network	CBMS-3	Entity receiving ESG information blocks (e.g. containers) from *one or more* logical ESG aggregators, putting them into FLUTE carousel(s) and optimizing mapping on DVB-H bursts (e.g. avoiding ESG information fragmentation over multiple bursts).
DVB-H resource manager	Broadcast Network	CBMS-6	*See description in service configuration section.*
IP-to-section mapper	Broadcast Network	CBMS-3	Entity in charge of encapsulating the IP datagrams into the DVB-H MPE sections and generate MPE-FEC sections by performing MPE-FEC encoding. Usually part of an IP encapsulator.
Service and content description handler	Terminal	CBMS-3	Receives and aggregates subset of or all ESG information blocks, maintains them up-to-date, and makes them available to the ESG application. *Presentation of and interaction with ESG information is out of scope of the present document.*

SDP files can be delivered as part of the ESG over the CBMS-3 reference point, but also may be delivered separately. SDP files are assumed to be created by the service application.

If delivered with the ESG, SDP files are delivered to the logical ESG aggregator via the CBMS-7 interface.

If delivered separately, the service application delivers the SDP file along with the content over the CBMS-2 reference point directly to the terminal.

5.2.2 Instantiation Scenarios

For a number of reasons, ranging from regulatory/legislative requirements to the need to adapt flexibly to different value chains, the architecture supports different instantiation scenarios with respect to the ESG provision. In the following, two of the possible instantiation scenarios are illustrated, each forming an extreme of the spectrum of scenarios possible.

5.2.2.1 Distributed ESG Provisioning

In this scenario each service application offered via the broadcast bearer provides the ESG independently and directly to the Terminal entity. The Service Guide client application on the terminal must process the multitude of ESG sources appropriately. This may happen by a merging process which results in a unified service guide presentation.

In this case the Service Guide Generation function coincides with the Service Guide Generation function in the Service Application Entity.

- ESG information is not logically aggregated (i.e. in a consistent way) in the head-end. The terminal has to do this step.
- Application providers at least specify delivery requirements to service management (bit rate, QoS parameters, time and duration, etc.).
- Application providers request bandwidth reservation for services to broadcast.

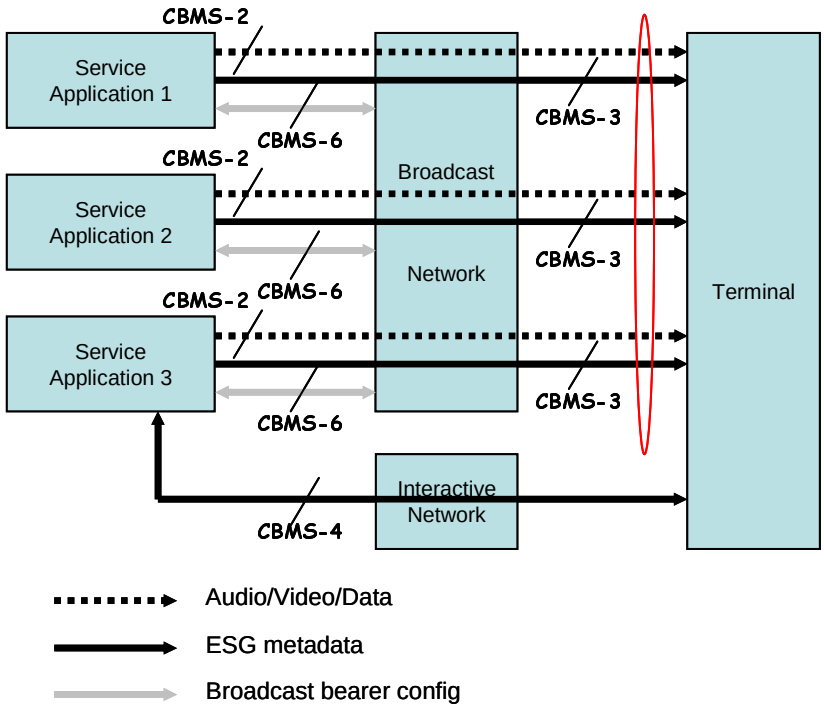

Figure 5: Distributed ESG provisioning

5.2.2.2 Centralized ESG Provisioning

In this scenario the Service Applications provide the ESG data to the Service Guide Provisioning function in the Service Management entity. The terminal receives all service guide information from a single source, the centralized Service Guide Provisioning function in the Service Management entity.

- Application providers or special aggregator provides ESG information.
- Application providers at least specify delivery requirements to service management (bit rate, QoS, time and duration, etc.).
- Service configuration requests bandwidth for services to broadcast.

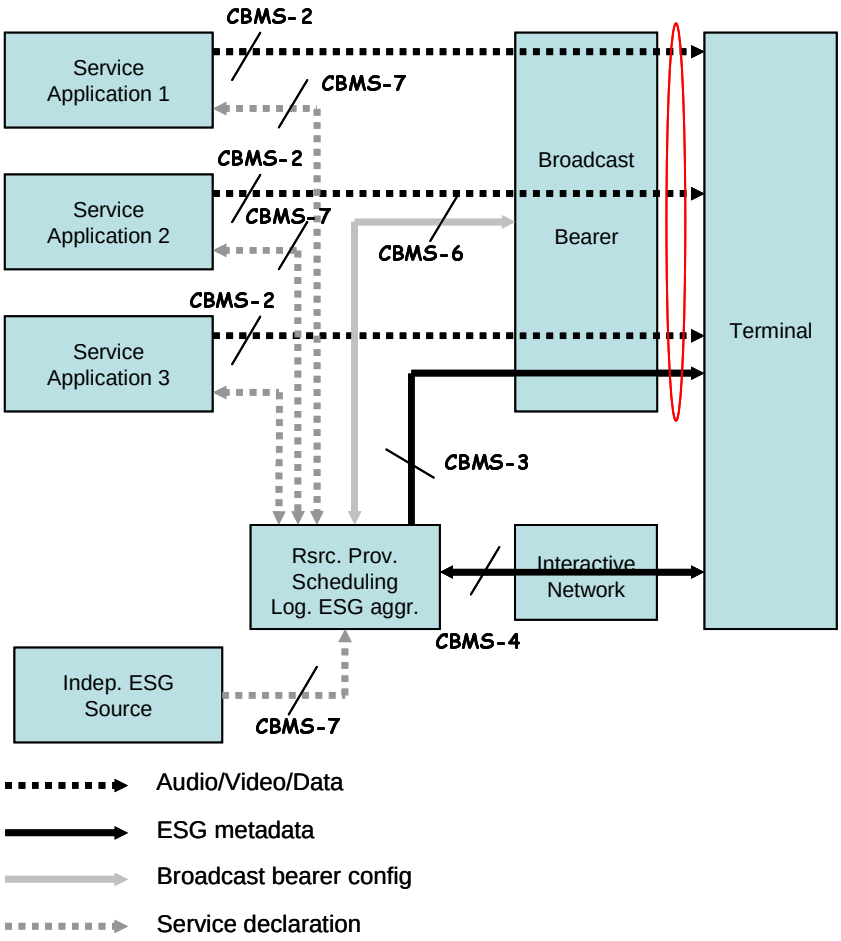

Figure 6: Centralized ESG provisioning

An example for an instantiation that has elements of both scenarios is the existence of a centralized Service Guide Provisioning function, but with additional, "independent" service guide providers, which may offer added value over the centralized provided service guide.

5.2.3 ESG bootstrapping

An IP platform may contain more than one electronic service guide. A well-known IP/port number combination is used in every IP platform to transport a service that announces all ESGs to be found in that IP platform. This is the *Bootstrap ESG Service*. The logical relationship between the Bootstrap ESG Service and the actual ESGs in a platform is show in figure 7.

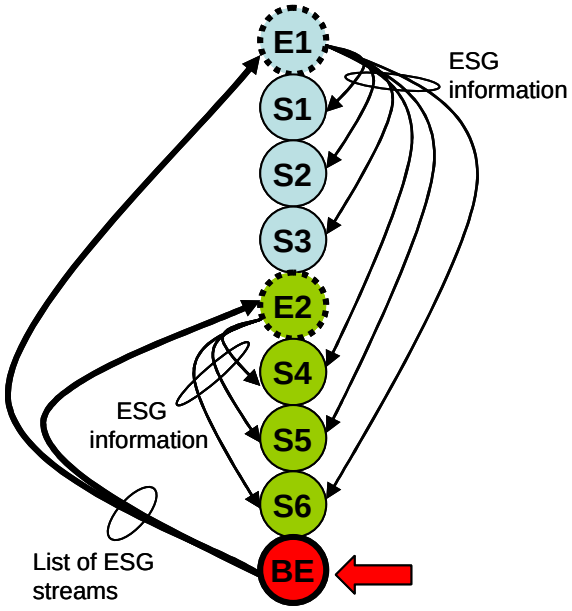

Figure 7: ESG Bootstrap Mechanism

- BE: Bootstrap ESG stream pointing to multiple ESGs (E1, E2). Bootstrap ESG information consists of *ESG provider descriptors* and related *ESG access descriptors* transported via FLUTE (ALC/LCT).
- ESGs (E1, E2) provide information about part or all of the available services (S1..Sn) (complete data model). The set of services described by each of the service guides may be disjoint, i.e. each service guide describes an exclusive set of services, or the set of services may overlap, as shown in figure 7.

5.2.3.1 Operational Considerations

- Both, actual and bootstrap ESG generation functions are service management functions.
- Bootstrap ESG generation is expected to be operated by IPDC platform operator.
- Bootstrap ESG generation function has to be aware of other ESGs to be delivered on the same platform.
- Actual ESG generation functions have to be aware of services to be delivered in platform (at least those the specific ESG describes).
- In the fully *distributed* instantiation scenario it may be useful to arrange the ESG information of each service together with the content delivery into the same time-slice burst and thus separate from the bootstrap ESG service.
  In the *centralized* instantiation scenario it may be useful to arrange the bootstrap ESG service and the actual ESG(s) into one time-slice burst. In that case, bootstrap ESG and actual ESGs may share the same destination IP address and are differentiated only by different destination port numbers.

5.2.3.2 ESG Bootstrap Procedure

The foreseeable way to retrieve a specific ESG within an IP platform would be as follows:

1. Retrieve INT for selected IP platform.
2. Search for PID with well-known IP address and port number for bootstrap ESG service.
3. Tune into this PID.
4. Retrieve Bootstrap ESG stream.
5. Select specific ESG by repeating steps 2 and 3 for the IP number of the selected ESG.
6. Retrieve selected ESG.

5.2.4 Message Flow

Figure 8 show the logical flow of messages between the entities/sub-entities involved.

The Message Sequence Chart assumes the following preconditions:

1. The logical ESG aggregator has configured itself using the message sequence for service configuration from clause 5.1.2 and thereby acting as a service application.

2. The service application has configured itself using the message sequence for service configuration from clause 5.1.2.

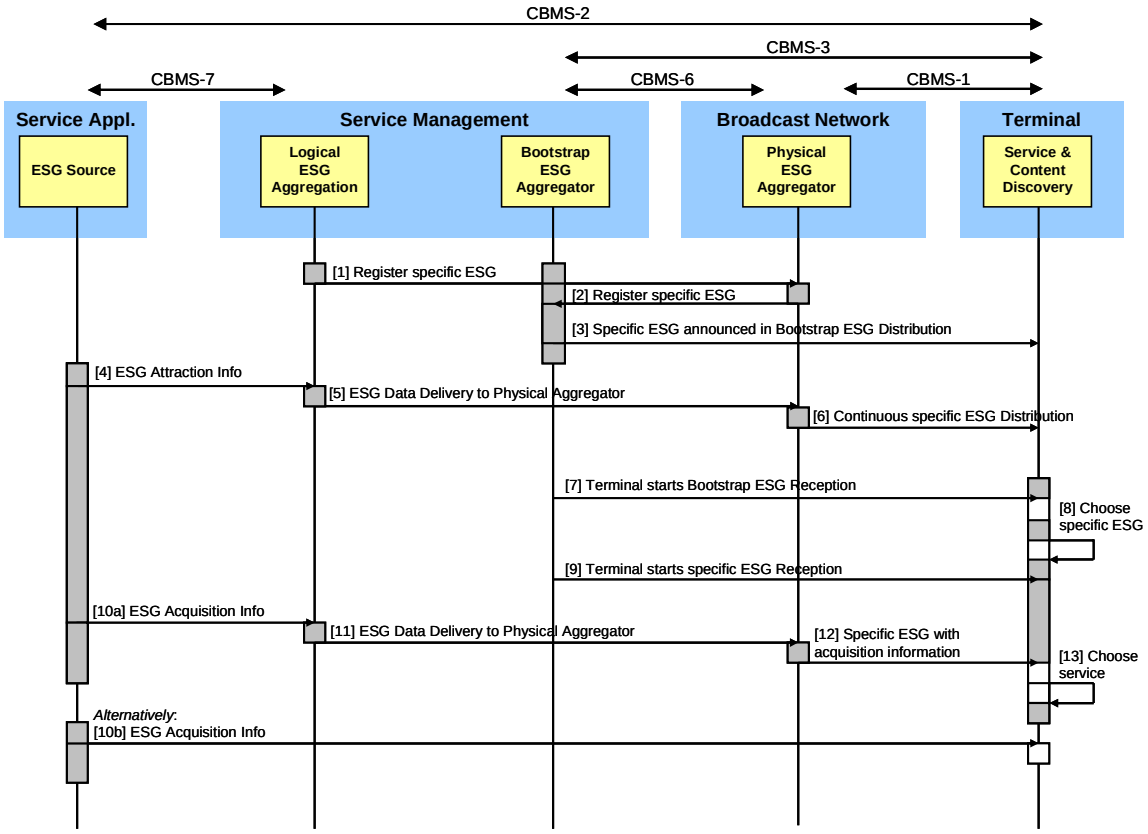

Figure 8: Interactions for ESG provisioning

Table 6 describes the messages shown in figure 8 in detail.

Table 6: Description of logical messages for ESG

1	**Register Specific ESG** The Logical ESG Aggregator registers itself with the Physical ESG Aggregator.
2	**Register specific ESG** As a result of specific ESG registration by message 1 the physical ESG Aggregator registers the specific ESG with the Bootstrap ESG Aggregator.
3	**Specific ESG announced in Bootstrap ESG Distribution** After registration of a specific ESG the Bootstrap ESG Aggregator includes it in its Bootstrap ESG distribution, transmitted to terminals.
4	**ESG Attraction Info** Service applications deliver attraction information to Logical ESG Aggregator. Service applications may do so at any time new attraction information becomes available.
5	**ESG Data Delivery to Physical Aggregator** As a result of ESG information delivery or update from Service Application (Attraction Information, message 4, or Acquisition Information, message 10), updated ESG data is delivered to the Physical ESG Aggregator.
6	**Continuous specific ESG Distribution** As soon as ESG data is available at the Physical ESG Aggregator, this ESG data is distributed to terminals.
7	**Terminal starts Bootstrap ESG Reception** At any point in time terminal(s) start to receive the Bootstrap ESG.
8	**Choose specific ESG** When having received the Bootstrap ESG, the terminal (with or without user interaction) chooses a specific ESG to receive. (It may want to receive more than one ESG.)
9	**Terminal starts specific ESG Reception** As a result of the choice of a specific ESG the terminal starts to receive it. The ESG delivery itself uses the file delivery mechanism described in clause 5.3.2. ESG information received is accumulated in a local ESG database.
10	**ESG Acquisition Info** At some point in time, but no later than the start of a service, the relevant acquisition information is delivered, either: to the Logical ESG Aggregator. It will then be included into the ESG. directly to the terminal (reference point CBMS-2).
11	**ESG Data Delivery to Physical Aggregator** See message 5. This message is issued after message variant 10a has been issued by the Service Application.
12	**Specific ESG with acquisition information** The Physical ESG Aggregator distributes the ESG updated with ESG Attraction Information if Service Application has chosen variant message 10a
13	**Choose Service** At some point in time, the terminal (with or without user interaction) has chosen a service to consume. It will then retrieve Acquisition Information from its ESG database and initiate the appropriate content consumption. The terminal SHOULD pass acquisition information (i.e. SDP file) and COULD pass service ID to content consumption. Using the service ID, content consumption can further refer to ESG information. This may also be useful to avoid double service activation in terminals. Content consumption uses Service Configuration Operation (see clause 5.1) to configure the service and Content Delivery Operation (see clause 5.3) for receiving content.

5.2.5 Operational Considerations

Configuration of the several sessions an ESG might be divided into. They may be arranged in the same or different time-slice bursts.

- In a use case where sessions are used specifically to convey in-depth information on a service, which is normally used when the service is actually consumed, it is useful to arrange such session(s) into the same burst as the actual service(s) it describes to allow simultaneous reception of content and in-depth service guide information.

- ESG information may be divided into sessions, where information on events in a more distant future is put into different ESG sessions. This allows such information to be cycled slower (reduced bandwidth) while other information can be obtained faster by the terminal.

5.3 Content Delivery

Consuming an IP Datacast service means that a terminal receives content and consumes it. There are two basic methods defined in IP Datacast to deliver content: Streaming and File Download, each of which is detailed in the next two clauses.

5.3.1 Stream Delivery

Real-time streaming is characterized as follows:

- The streamed data is intended to be consumed as it is received. This does neither preclude buffering nor optional (long-term) storage of the data stream.
- The data is received in real-time, i.e. with a close timely relationship to its consumption/presentation.
- A receiver may start at any point in time (after the stream transmission has started) to receive the stream. Also, the receiver may stop at any time to receive the stream.

Data types for streaming that are defined in the scope of the IP Datacast over DVB-H specification, comprise:

- Video.
- Audio.
- Subtitling.

Encoding formats for video and audio are specified in annex B of [13].

5.3.1.1 Logical Entities and Reference Points

Figure 9 identifies sub-entities of the main entities introduced in clause 4 that are involved for the stream delivery operation. It also highlights the reference points that are involved in this operation.

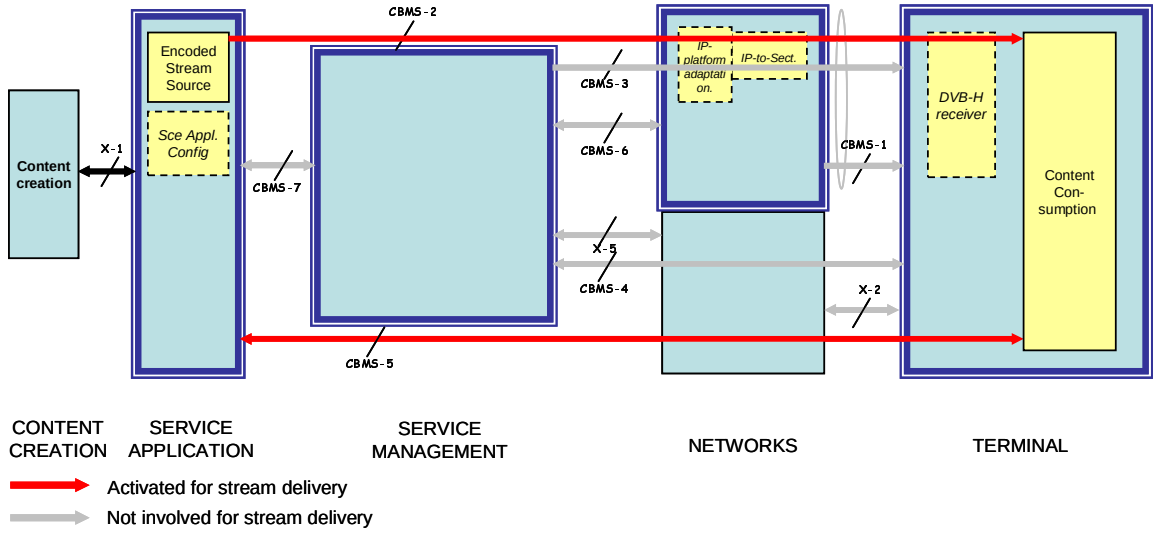

Figure 9: Reference points activated for stream delivery

Table 7 describes the sub-entities introduced in figure 9.

Table 7: Description of logical sub-entities involved in stream delivery

Logical sub-entity	Logical Entity it is part of	Involved Ref. Points	Description
Encoded stream source	Service Application	CBMS-7, CBMS-5	Entity outputting media streams (e.g. Audio, Video, Data) towards broadcast networks, using configuration parameters obtained from *service application configuration* sub-entity.
Content Consumption	Terminal	CBMS-7, CBMS-5	Entity processing the received media stream; it may include facilities for buffering, synchronization, storing, and rendering of the stream content.
IP platform adaptation	Broadcast Network	CBMS-2, CBMS-3, CBMS-6, CBMS-7	Entity in charge of adapting payload traffic sources into IP platforms as defined by DVB-H service handler on behalf of resource provisioning and scheduling. IP platform adaptation may perform gateway functions from the contribution network to the broadcast distribution network. This includes: • Firewall/Source authentication. • Address translation from IPv4 to IPv6 or vice versa. • Unicast to multicast translation. • TCP to UDP translation or tunnelling. The service application must be informed about the adaptation function, so it can set up SDP files correctly (for source and destination addresses, port numbers, protocols). Reference points CBMS-7 and CBMS-6 are involved for that. This is subject of further study for DVB-CBMS.

5.3.1.2 Message Flow

Figure 10 shows the logical flow of messages between the entities/sub-entities involved.

The Message Sequence Chart assumes the following preconditions:

1) The application has configured itself using the message sequence for service configuration from clause 5.1.2.

2) The terminal may have used the ESG to discover and choose the service using the message sequence from clause 5.2.4.

3) The terminal has configured for receiving the service using the message sequence for service configuration from clause 5.1.2.

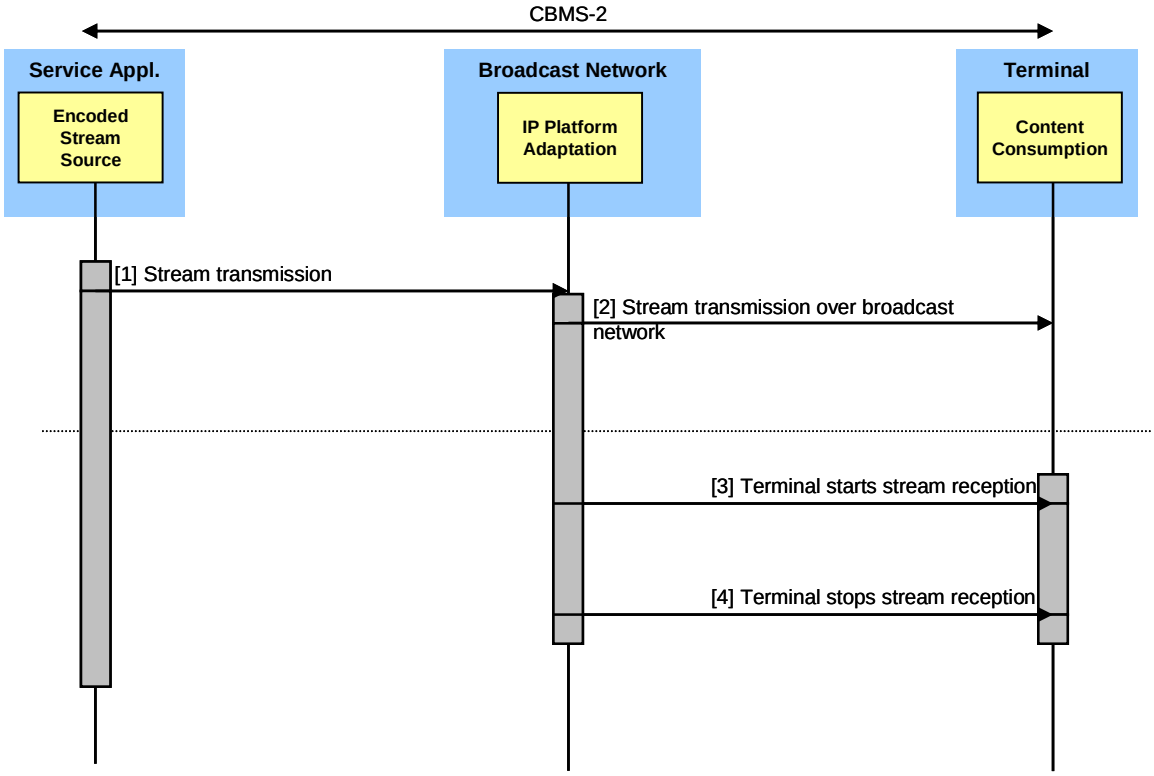

Figure 10: Message flow for Stream Delivery

In the message flow shown in figure 10 the IP-to-section mapping sub-entity and the IP Receiver do not occur, since they are transparent in this operation.

Table 8 describes the messages shown in figure 10 in detail.

Table 8: Description of logical messages for Stream Delivery

1	**Stream transmission** The Service Application's Stream Source starts to stream the encoded content to the IP Platform Adaptation.
2	**Stream transmission over broadcast network** As a result of message 1, the stream is transmitted over the broadcast network to terminals.
3	**Terminal starts stream reception** At some point in time, the terminal starts reception of the stream. The stream is directed to the Content Consumption.
4	**Terminal stops stream reception** At any point in time, the terminal stops the stream reception.

5.3.2 File Delivery

File delivery is characterized as follows:

- Unlike a real-time stream, all the file data are to be first received and stored into the terminal before being used by appropriate applications.
- To ensure the completeness and integrity of received files, a unidirectional file delivery protocol is used. In addition to that, post delivery repair mechanisms may be defined by the operator, which may or may not use the interaction channel.

5.3.2.1 Logical Entities and Reference Points

Figure 11 identifies sub-entities of the main entities introduced in clause 4 that are involved for the file delivery operation. It also highlights the reference points that are involved in this operation.

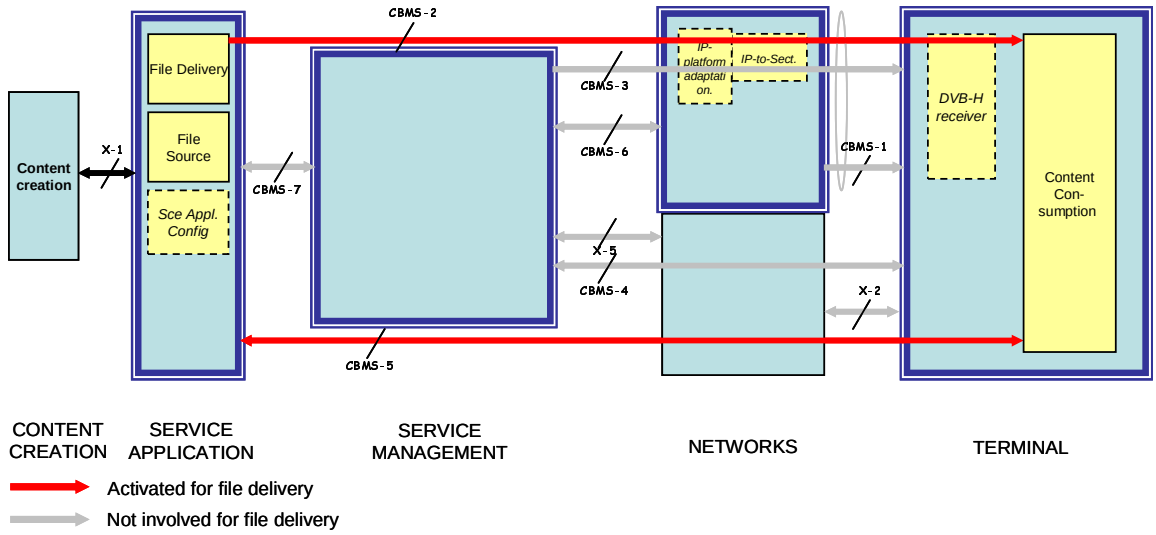

Figure 11: Reference points activated for file delivery

Table 9 describes the sub-entities introduced in figure 11.

Table 9: Description of logical sub-entities involved in file delivery

Logical sub-entity	Logical Entity it is part of	Involved Ref. Points	Description
File source	Service Application	Internal to SA	Entity generating file content to be transferred to terminals.
File delivery	Service Application	CBMS-7, CBMS-5	Entity generating file delivery sessions, e.g. a file carousel server. It also may contain the post repair server.
Content Consumption	Terminal	CBMS-7, CBMS-5	Entity processing the received media stream; it may include facilities for buffering, synchronization, storing, and rendering of the stream content.

5.3.2.2 Message Flow

Figure 12 shows the logical flow of messages between the entities/sub-entities involved.

The Message Sequence Chart assumes the following preconditions:

1) The application has configured itself using the message sequence for service configuration from clause 5.1.2.

2) The terminal may have used the ESG to discover and choose the service using the message sequence from clause 5.2.4.

3) The terminal has configured for receiving the service using the message sequence for service configuration from clause 5.1.2.

4) The File Delivery has started the (maybe indefinite) file delivery session.

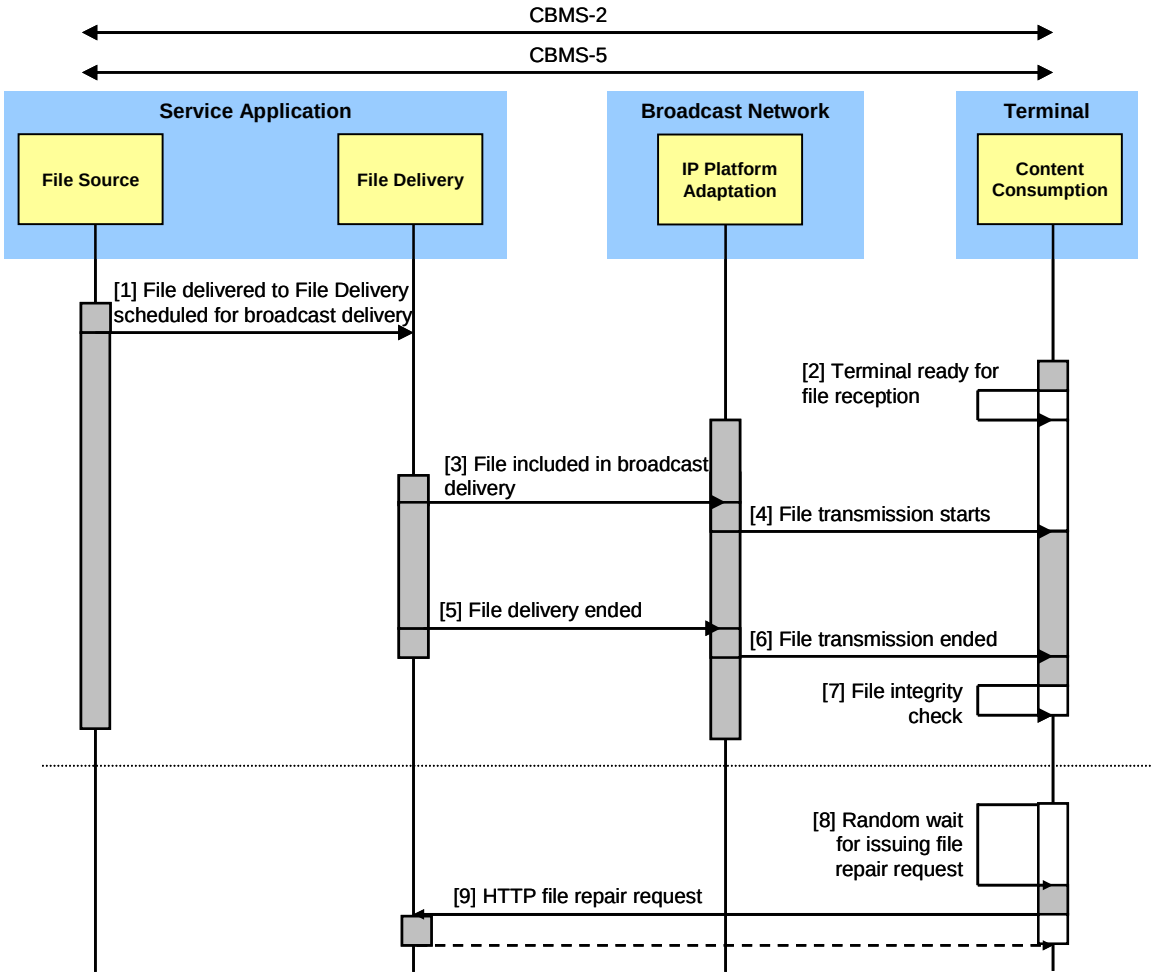

Figure 12: Message flow for File Delivery

In the message flow shown in figure 12 the IP-to-section mapping sub-entity and the IP Receiver do not occur, since they are transparent in this operation.

Table 10 describes the messages shown in figure 12 in detail.

Table 10: Description of logical messages for File Delivery

1	**File delivered to File Delivery scheduled for broadcast delivery** The File Source delivers a file to the File Delivery and specifies scheduling and perhaps additional delivery parameters.
2	**Terminal ready for file reception** The terminal configures for file delivery session reception and waits for file(s) to be transmitted.
3	**File included in broadcast delivery** As a result of message 1, when the scheduled time for file delivery has arrived, the file is included in the file delivery session. The session output is directed to the IP Platform Adaptation.
4	**File transmission starts** After IP Platform Adaptation the file delivery session including the file added in message 3 is transmitted via the broadcast channel to terminals.
5	**File delivery ended** In the file delivery session, eventually the delivery of a file is ended.
6	**File transmission ended** As a result of message 5, in the file delivery session transmission, transmission of the file has ended.
7	**File integrity check** When the file transmission is ended, the terminal checks the file for integrity/completeness by using checksums provided by the file delivery session. Two different file post repair mechanisms are defined: A broadcast file post repair session. If this is used by the terminal, the same message sequence is used again for the post repair session. A post repair server may be specified, which can be used if the terminal has an endpoint for the interaction channel.
8	**Random wait for issuing file repair request** If an interactive post repair server is signalled in the file delivery session, and a file is considered incomplete or corrupt by the terminal, and the terminal has an endpoint for an interaction channel, it has to wait a random period before it issues the repair request message 9. This helps to reduce the contention for accessing the post repair server.
9	**HTTP file repair request** The terminals issues a HTTP request for the parts of the file it is missing or are corrupt. The response may be one of the following: The missing parts in the response message body. In that case the file reception is complete. Redirection to a different repair server. In that case the terminal issues the same HTTP message to the different repair server. Redirection to a broadcast repair session, indicated by a redirection message to the SDP file for the repair session. In that case the terminal starts to use the repair session using the message flow described here. An error message.

5.3.2.3 Operational Considerations

The File Delivery sub-entity is logically part of the service application(s). For practical reasons, this sub-entity may be operated by the broadcast network operator.

5.4 Service Purchase and Protection

The IP Datacast over DVB-H specification includes a specification for Service Purchase and Protection [12], which contains three methods for content/service encryption and two system approaches for the other elements needed. In the following the architectural integration for service purchase and protection is described, as far as it is applicable to both of them.

5.4.1 Hierarchical Service Protection Model

Figure 13 presents the hierarchical model for service protection.

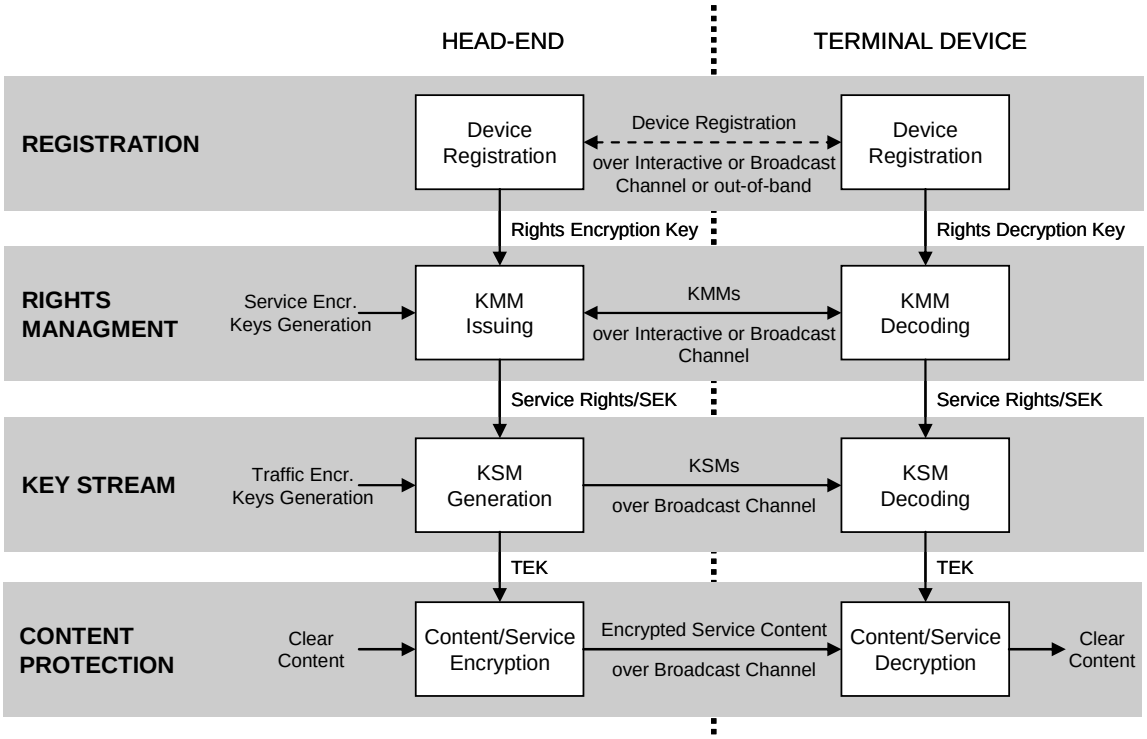

Figure 13: Hierarchical Model for Service Protection

Registration

Key material and metadata are exchanged during the registration phase that will enable terminal devices to decrypt and authenticate rights and subsequently access content.

Rights Management

In the rights management layer Key Management Messages (KMM) are furnished e.g. as a result of a purchase transaction and transferred to terminals via the interactive or broadcast channel. These may contain a Service Encryption Key (SEK) or information such as entitlements.

Key Stream

This layer implements the delivery of Traffic Encryption Keys (TEK) by transmission of Key Stream Messages (KSM) to the terminal on the broadcast channel. These messages in essence contain information that allows the terminal to reconstruct the Traffic Encryption Keys (TEK) needed to decrypt the service content. ECMs/KSMs may contain additional information to control the service access, such as access criteria.

Content Protection

The Service Content is encrypted by a symmetric encryption algorithm with a Traffic Encryption Key (TEK). The encryption can be performed on link layer (IPSec), session layer (e.g. SRTP), or content layer (e.g. ISMACryp). Traffic Encryption Keys change frequently to prevent real-time key distribution attacks.

5.4.2 Logical Entities and Reference Points

Figure 14 identifies sub-entities of the main entities introduced in clause 4 that are involved for the ESG operation. It also highlights the reference points that are involved in this operation.

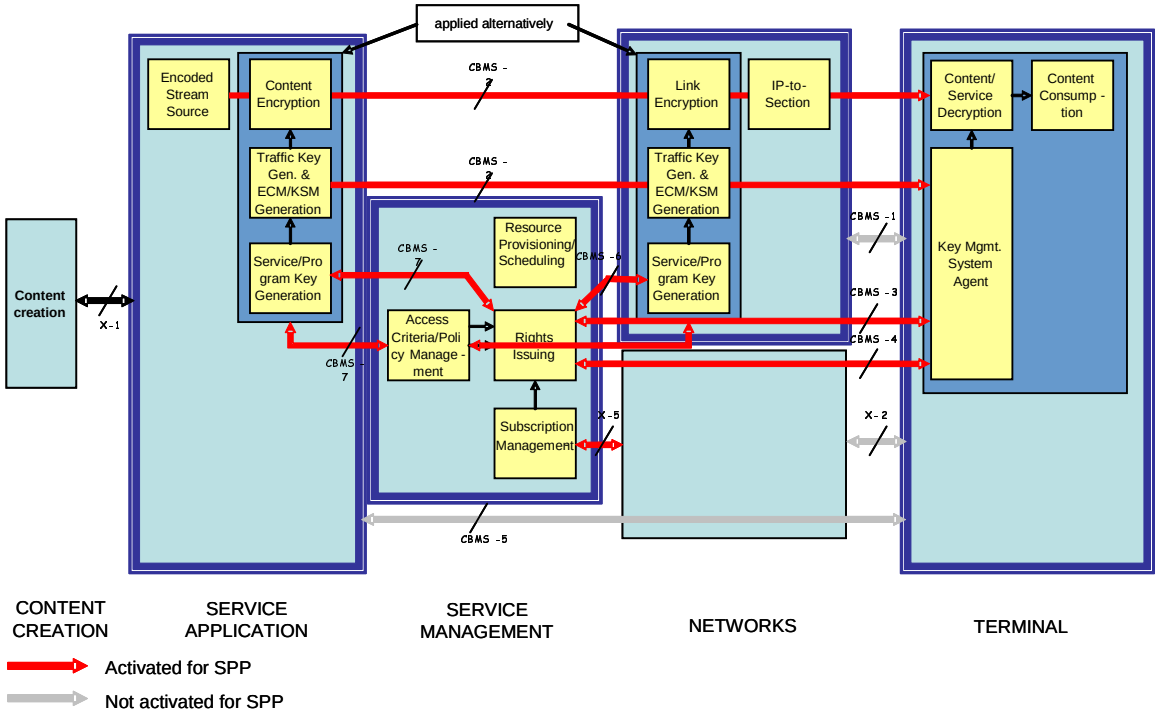

Figure 14: Sub-Entities and reference points activated for Service Purchase and Protection

The dark boxes surrounding the security sub-entities inside Service Application, Broadcast Network indicate a secure environment for these sub-entities. In the Terminal it indicates a secure processing/storage environment for these sub-entities.

Table 11: Description of logical sub-entities involved in Service Purchase and Protection

Logical sub-entity	Logical Entity it is part of	Involved Ref. Points	Description
Encoded stream source	Service Application	CBMS-2	Entity outputting media streams (e.g. Audio, Video, Data) towards broadcast networks, using configuration parameters obtained from *service application configuration* sub-entity.
Content Encryption	Service Application	CBMS-2	Entity in charge of encrypting the content stream. Content encryption and link encryption need not to be used simultaneously.
Link Encryption	Broadcast Network	CBMS-2	Entity in charge of encrypting the data stream at the link level. This type of encryption is agnostic of the service content. Content encryption and link encryption need not to be used simultaneously.
Traffic Key Generation and ECM/KSM Generation	Service Application *or* Broadcast Network	CBMS-2	This entity generates the Traffic Encryption Keys for content or link traffic, respectively. TEKs are frequently changed.
Service/Program Key Generation	Service Application *or* Broadcast Network	CBMS-7	This entity generates the keys for service/program access. It is controlled by the Service Management's Access Criteria/Policy Management sub-entity. Service/Program keys are exchanged with Rights Issuing sub-entity in Service Management.
IP-to-section	Broadcast Network		See table 5.
Access Criteria/Policy Management	Service Management	CBMS-7, CBMS-6	This entity may define services, programmes, and their lifetimes, which bundles of media flows they contain and the access criteria to the content. May also define purchasable items, such as service bundles.
Rights Issuing	Service Management	CBMS-3, CBMS-4, CBMS-6, CBMS-7	This entity furnishes rights messages for delivery to the terminal's Key Management System Agent. This process may require access criteria, service/programme keys, and the result of a successful purchase transaction. The latter is managed by the Subscription Management sub-entity.
Subscription Management	Service Management	X-5 (opt.)	This entity manages the specifics of each end user's subscription. It may use the interactive network's billing function over the X-5 reference point or other, independently operated billing systems. The billing function, however, is out of scope of the present document.
Resource Provisioning/ Scheduling	Service Management		*See table 3. Used here for configuration of KSM delivery.*
Content/Service Decryption	Terminal	CBMS-2	This entity decrypts content/link traffic with the TEKs the Key Management System Agent provides.
Key Management System Agent	Terminal	CBMS-2, CBMS-3, CBMS-4	This entity receives and manages Rights messages and Key Stream Messages. If all criteria for entitlement match, the TEK is reconstructed and provided to the Content/Service Decryption entity.
Content consumption	Terminal	CBMS-2	Entity processing the received media stream; it may include facilities for buffering, synchronization, storing, and rendering of the stream content.

5.4.3 Message Flow

Figure 15 shows the logical flow of messages between the entities/sub-entities involved.

The Message Sequence Chart assumes the following preconditions:

1) The application has configured itself using the message sequence for service configuration from clause 5.1.2.

2) The terminal may have used the ESG to discover and choose the service using the message sequence from clause 5.2.4.

3) The terminal has acquired appropriate rights for consumption of the stream, which are managed by the terminal's Key Management System Agent. The message sequence to acquire rights is out of scope of the present document.

4) The terminal has configured for receiving the service using the message sequence for service configuration from clause 5.1.2.

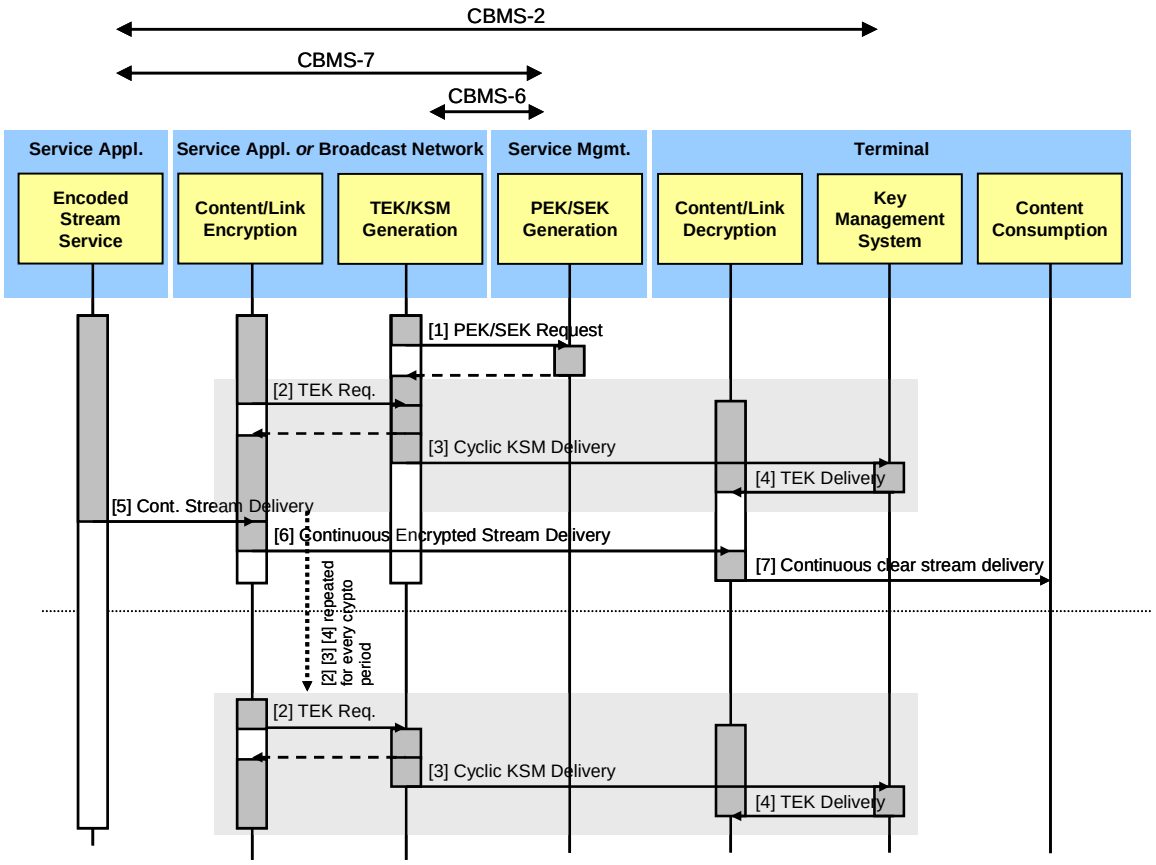

Figure 15: Interactions for Service Purchase and Protection

Table 12 describes the messages shown in figure 15 in detail.

Table 12: Description of logical messages for Service Purchase and Protection

1	**PEK/SEK Request** Key Stream Message Generator requests the programme/service key from Programme/Service Key Generator. The SEK is responded back to the KSMG.
2	**TEK Request** The Content/Link Encryption requests the current TEK from the key generator part of the Traffic Key Generator/KSM Generator. The TEK is responded back to the Content/Link Encryption.
3	**Cyclic KSM Delivery** After starting generation of TEKs, key stream messages are repeatedly transmitted to terminals, where they are directed to KSMA.
4	**TEK Delivery** The TEK is delivered by the KSMA to the Content/Link Decryption in the terminal, if the KSMA has verified proper entitlement for content access.
5	**Stream Delivery** The Encoded stream Source starts to send the content to the Content/Link Encryption.
6	**Encrypted Stream Delivery** After encrypting the stream with the TEK obtained in message 2 it is transmitted to terminals, where it is directed to Content/Link Decryption.
7	**Clear Stream Delivery** After decryption, the clear stream is delivered to the Content Consumption.

The message sequence for the rights issuing process is highly dependent on the specificities of the key management system actually used. Therefore it is not covered in the present document.

6 Protocol Stack

The following clause describes the protocol hierarchy for the air interface including reference points CBMS-1 to CBMS-5. Other reference points related to Service Management and Service Application will be mapped to the protocol hierarchy in phase 2 of the specification. In difference to the ISO/OSI Layering Model, in figure 16 a section for Enabling Services is introduced to the protocol hierarchy.

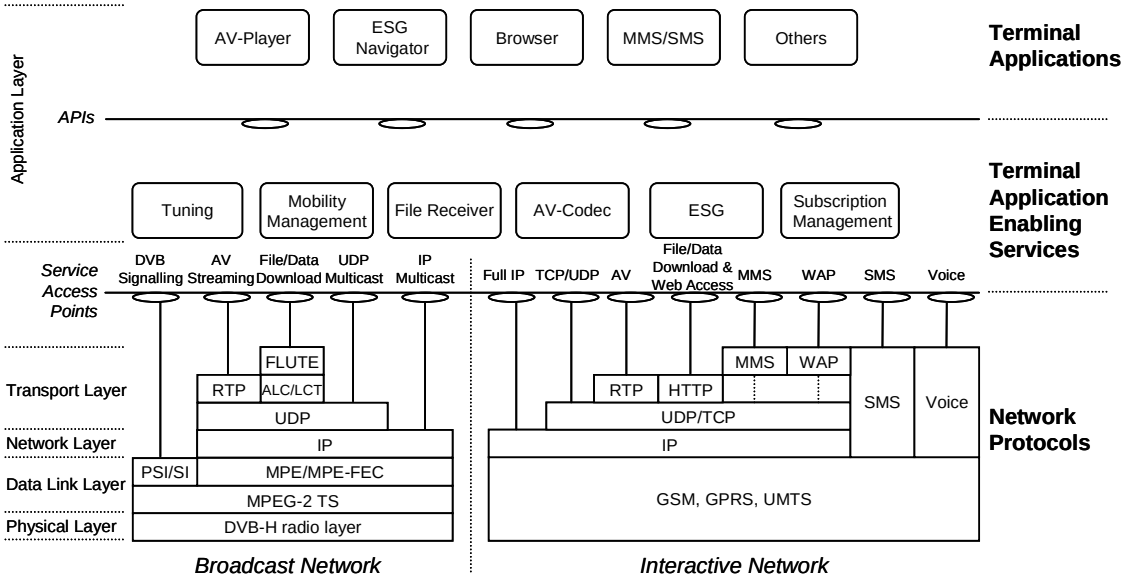

Figure 16: Protocol, Enablers, Applications Hierarchy in IP Datacast

Tables 13 and 14 describe the service access points (see clause 3.1) shown in figure 16.

Table 13: Definition of service access points on the broadcast network

Service Access Points on the *broadcast* network	Description
DVB Signalling	Access point mainly used by tuning and mobility management enablers to obtain relevant configuration information.
AV Streaming	Access Point for all Audio/Video streams delivered over the Broadcast network
File/Data Download	Access Point for all data delivered over the Broadcast network via FLUTE (one time or carousel based)
IP Multicast	Access point to IP multicast for application specific usage of IP multicast.
UDP Multicast	Access point to UDP multicast for application specific usage of IP multicast datagram services.

Table 14: Definition of service access points on the interactive network

Service Access Points on the *interactive* network	Description
Full IP	Access Point for all other IP-based point-to-point communication over the cellular network
Full TCP/UDP	Access Point for all other IP-based point-to-point stream and datagram communication over the cellular network
File/Data Download and Web Access	Access point for file delivery repair services and general web access.
AV	Access Point for all Audio/Video streams delivered over the cellular network
MMS	Access Point for receiving and sending Multimedia Messages
WAP	Access Point for the access of WAP Services
SMS	Access Point for receiving and sending Short Messages.
Voice	Access Point for Voice Calls

Table 15 describes the application enabling services shown in figure 16. These are application elements that enable an application to be built on top of IP Datacast service. The application enabling service may consist of an element in the terminal and/or a counterpart in the head-end.

Table 15: Definition of enabling services

Enabling Services	Description
Subscription Management (optional)	Subscription Management manages rights acquisition and keeps track of rights acquired for the terminal and controls the decryption process of service content in the terminal.
Tuning	Basic frequency tuning and scanning, selection of IP platform, tuning to PIDs of multicast IP addresses selected by the terminal, basic handover support for Mobility Management.
AV-Codec	On the terminal side, enables decoding and rendering of Audio/Video content. On the head-end, takes care of encoding Audio/Video content.
ESG	Receive Electronic Service Guide(s), maintains ESG cache, notification of ESG-using applications of updates.
File receiver	File carousel receiver and management of received files. Post-delivery repair of incomplete received files. Notification of file-consuming applications of new file arrivals and updates.
Mobility Management	Enables Handover and Roaming functionality.

Table 16 informatively describes IPDC terminal applications show in figure 16.

Table 16: Terminal applications

Applications	Description
AV-Player (optional)	Enables the functionality to play Audio and Video files and streams. (There may be terminals dedicated to the delivery of files only.)
ESG Navigator (optional)	Enables the presentation of and the interaction with one or more ESGs from one or more Service Providers
Browser (optional)	Enables the functionality of browsing pages (e.g. web pages)
MMS/SMS (optional)	Enables the presentation of MMS/SMS on the end-user-terminal
Others (optional)	May include other applications like games, etc.

7 Map of IP Datacast specifications

This clause is to provide a mapping of all of the IP Datacast over DVB-H specifications to:

- The logical entities and reference points of the architecture.
- The protocol stack.

In that it is actually serving as a map laying out all specifications and giving an overview of all the specifications (inside and outside of DVB) that IP Datacast over DVB-H is referencing.

7.1 CBMS-1

Reference point CBMS-1 between broadcast network and terminal. It is used to signal IP streams over the broadcast bearer.

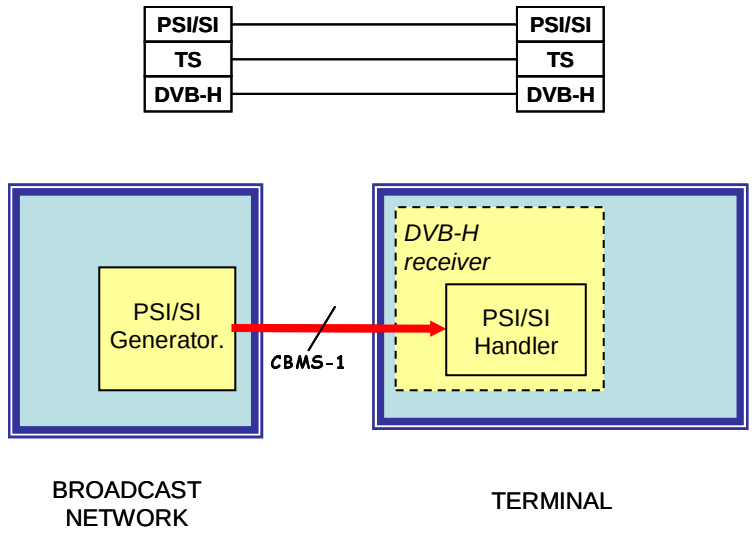

Figure 17: Protocols over reference point CBMS-1

These protocols are subject of TS 102 470 [11].

7.2 CBMS-2

Reference point CBMS-2 between service application and terminal. It is used for content delivery over the broadcast network. Both, Stream Delivery and File Delivery are considered in figure 18.

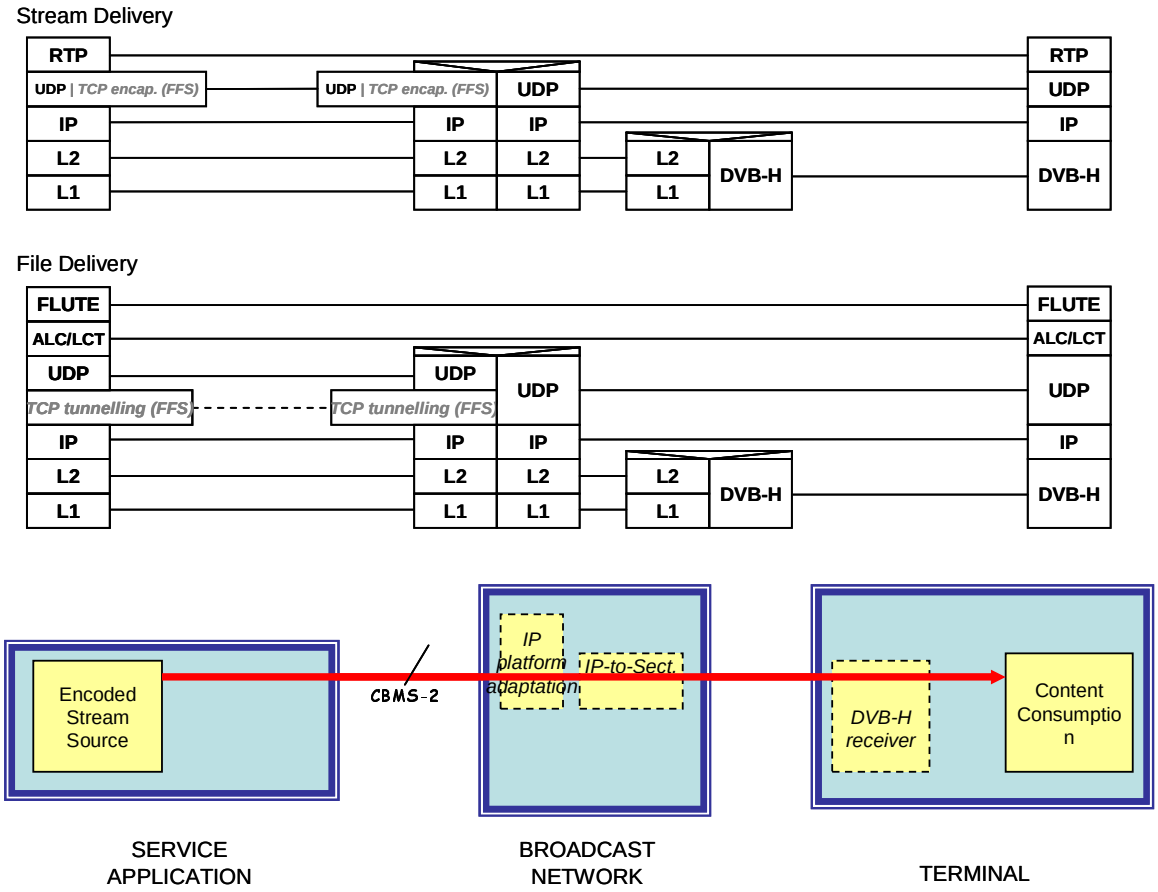

Figure 18: Protocols over reference point CBMS-2

Figure 18 indicates that at the contribution side for streams an encapsulation may be used as part of the head-end interface. This is subject of further study. An RTP in TCP encapsulation method is defined in subclause 10.12 of RFC 2326 [14].

These protocols are subject of TS 102 472 [10].

7.3 CBMS-3

Reference point CBMS-3 between service management and terminal. The ESG is delivered on this reference point.

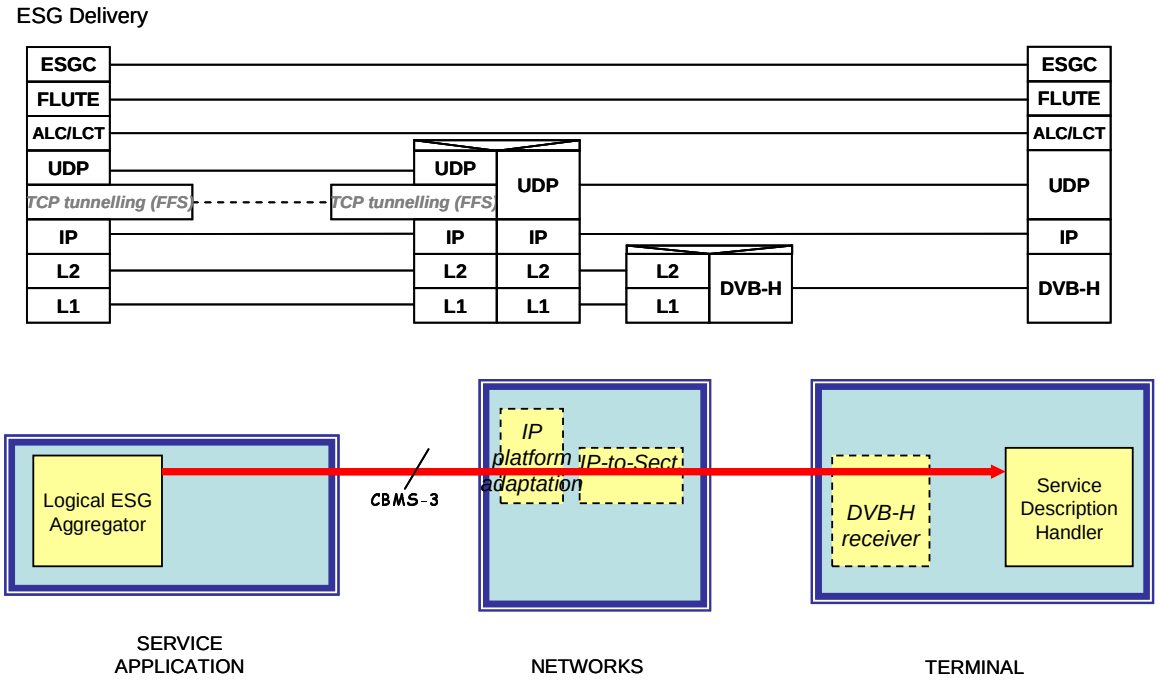

Figure 19: Protocols over reference point CBMS-3

ESGC: Encoded ESG information is transported in ESG fragment containers. L4/L5 protocol levels at the head-end side are subject of further study.

The ESG is subject of document 'IP Datacast over DVB-H: Electronic Service Guide (ESG)' [9], the FLUTE/ALC/LCT delivery protocols are subject of TS 102 472 [10].

7.4 CBMS-4

Reference point CBMS-4 between service management (Logical ESG Aggregator) and terminal (Service and content description handler) over the interaction channel. This reference point is optional. If available in the Terminal and configured for in the Service Management, it is used for ESG post delivery repair.

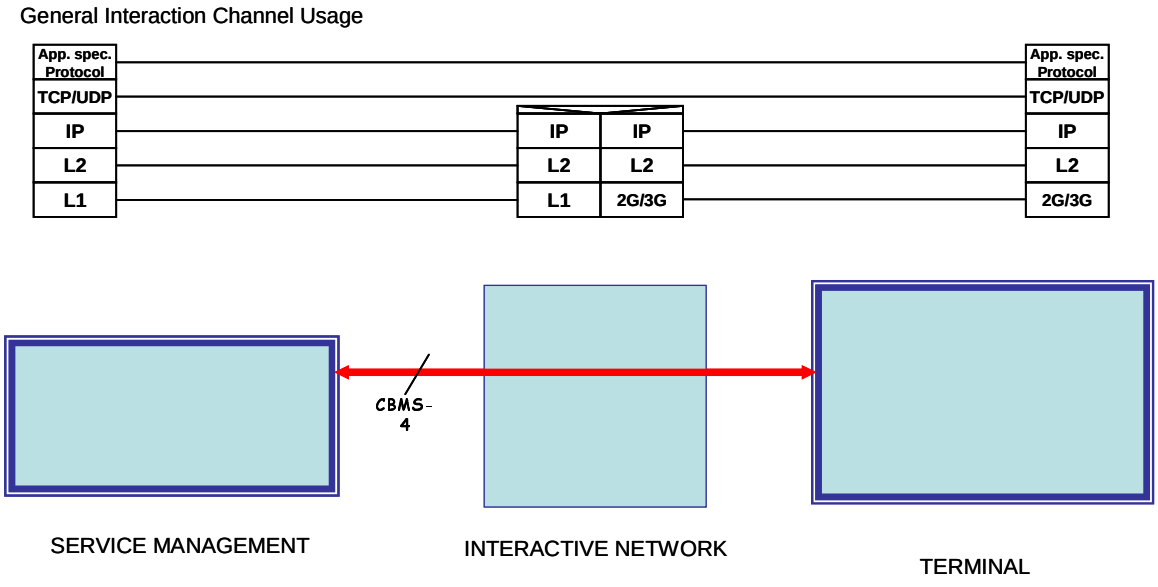

Figure 20: Protocols over reference point CBMS-4

This reference point may be used e.g. to retrieve ESG information via the interaction channel. The current IP Datacast over DVB-H specification does not yet provide for this. This is for further study.

7.5 CBMS-5

Reference point CBMS-5 between service application and terminal via the interaction network. This reference point is optional for terminals. It is used for general interaction between terminal service applications. In IP Datacast only for File Post Delivery Repair it is defined up the application level.

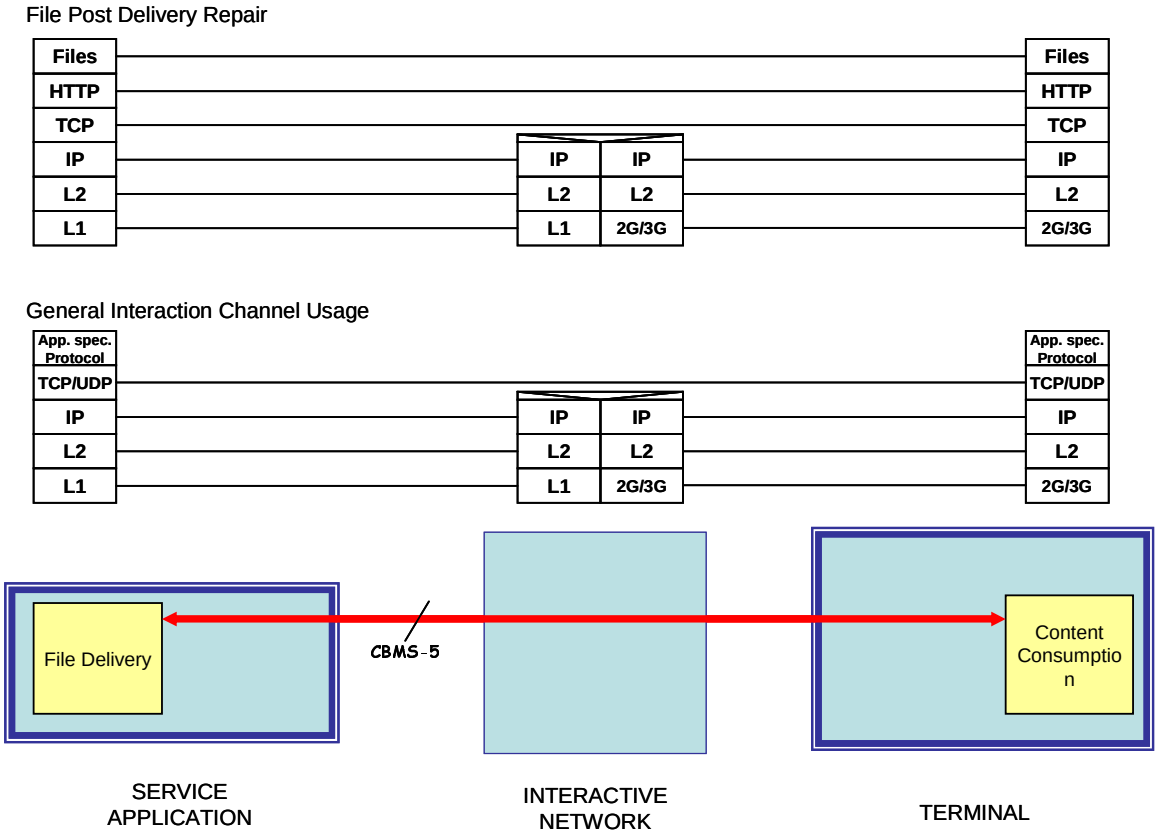

Figure 21: Protocols over reference point CBMS-5

File Post Delivery Repair is subject of TS 102 472 [10].

7.6 CBMS-6

Reference point CBMS-6 between service management (resource provisioning and scheduling) and broadcast network (DVB-H service handler).

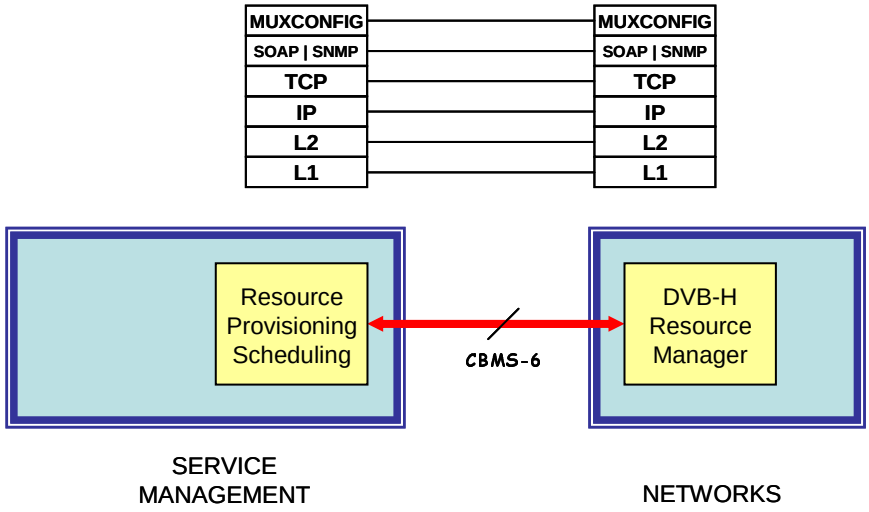

Figure 22: Protocols over reference point CBMS-6

CBMS-6 comprises head-end interfaces that are subject of further study. Therefore, mention of Muxconfig, SOAP, and SNMP are non-normative and just indicative for future specification work.

7.7 CBMS-7

Reference point CBMS-7 between service application and service management.

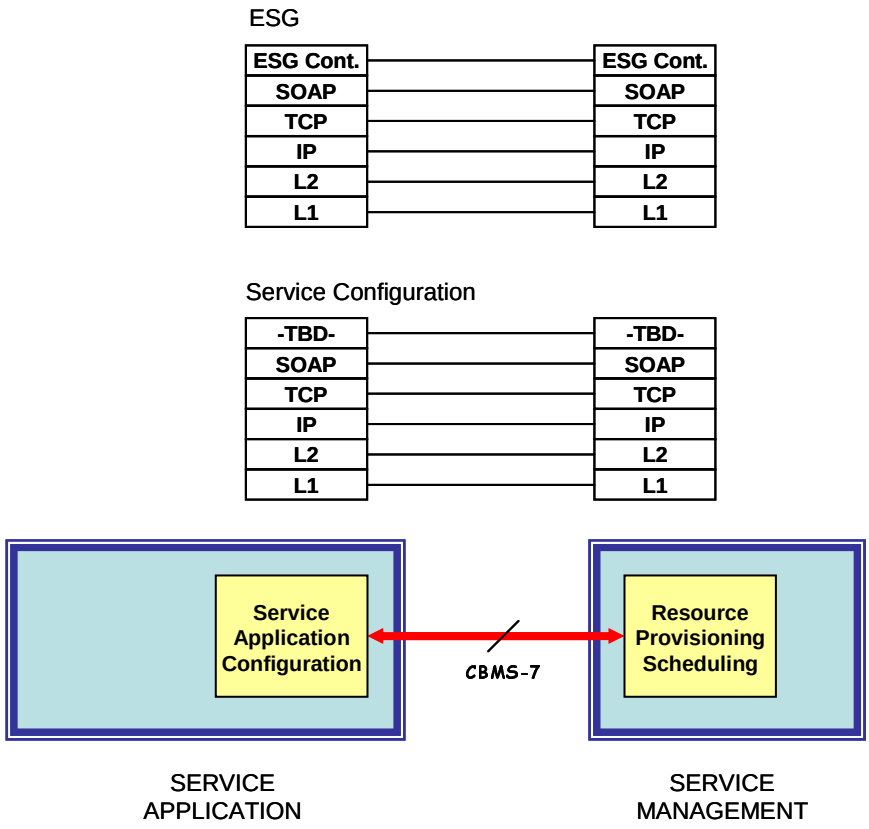

Figure 23: Protocols over reference point CBMS-7

CBMS-7 comprises head-end interfaces that are subject of further study. Therefore, mention of SOAP is non-normative and just indicative for future specification work.

History

Document history		
V1.1.1	May 2006	Publication