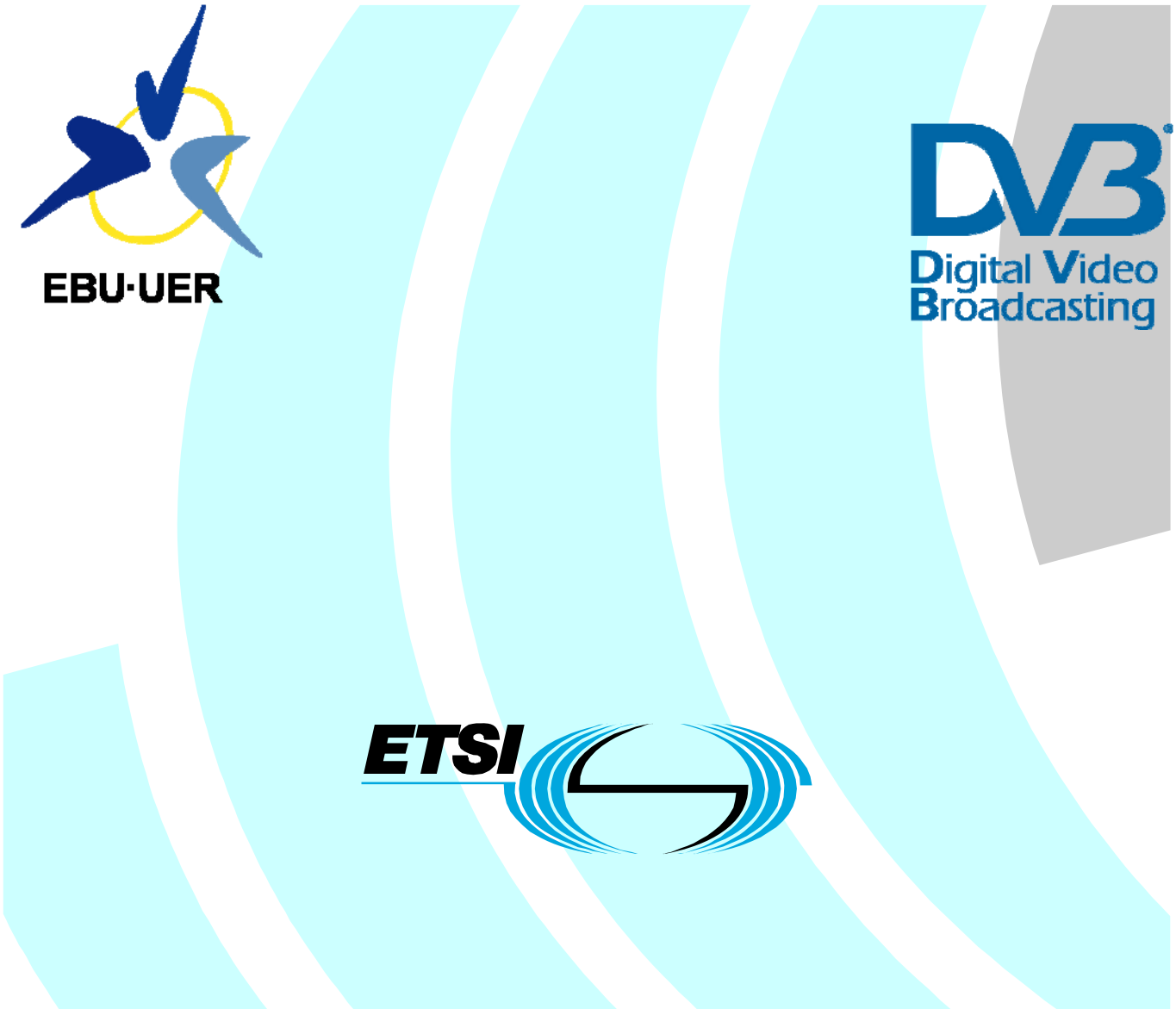
ETSI TS 102 542-4 V1.3.2 (2011-05)

Technical Specification

Digital Video Broadcasting (DVB); Guidelines for the implementation of DVB-IPTV Phase 1 specifications; Part 4: Remote Management and Firmware Update



Reference
RTS/JTC-DVB-303-4

Keywords
broadcasting, digital, DVB, IP, TV, 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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

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

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

Foreword

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

Please note that the present document is a revision to TR 102 542, and has been converted to a TS because the language used in the document is akin to that of a TS.

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

The Digital Video Broadcasting Project (DVB) is an industry-led consortium of broadcasters, manufacturers, network operators, software developers, regulatory bodies, content owners and others committed to designing global standards for the delivery of digital television and data services. DVB fosters market driven solutions that meet the needs and economic circumstances of broadcast industry stakeholders and consumers. DVB standards cover all aspects of digital television from transmission through interfacing, conditional access and interactivity for digital video, audio and data. The consortium came together in 1993 to provide global standardisation, interoperability and future proof specifications.

The present document is part 4 of a multi-part deliverable full details of the entire series can be found in part 1 [i.1].

Introduction

Remote management and firmware update service 1s specified in TS 102 824 [2] as an optional extension to the DVB IPTV service covered by TS 102 034 [1].

The present document describes the implementation of specific capabilities of the RMS-FUS architecture where it was felt that TS 102 824 [2] may provide insufficient clarity or information. It should not be considered that the present document can be used in isolation from TS 102 824 [2].

1 Scope

The present document can not be considered as a complete specification for or description of the Remote Management and Firmware Update System specified by DVB, it is created to provide guidance to be used in conjunction with the specification (TS 102 824 [2]) in association with TS 102 034 [1].

TS 102 824 [2] describes the functionality required to support three primary usage models:

- RMS-only - management and firmware maintenance of CPEs within a managed environment, the presence of a Remote Management Server is assumed in the logical head-end network architecture but no Firmware Update Server is needed.
- FUS-only - the provision of a generic firmware update service (FUS) which can be accessed by unmanaged CPEs, the service is assumed to be provided by a Firmware Update Server in the logical head-end system without using a Remote Management Server and may be supported directly or indirectly by the CE manufacturer.
- RMS-FUS combination - the provision of a generic firmware update service which can be controlled by a remote management service (RMS) for the managed population of CPEs. Because the system is considered in a completely logical way the same FUS may also provide firmware updates for unmanaged CPEs.

TS 102 824 [2] is designed to be used in conjunction with the DVB IPTV Handbook TS 102 034 [1] and these guidelines are focused on the solutions that can be realised using the combination of these specifications. However, TS 102 824 [2] may be used in other environments besides those described by TS 102 034 [1] where suitable methods are provided to link between the environment and the RMS and FUS sub-systems.

The present document includes:

- Some description of the system reference model, including the interfaces is introduced in clause 4.
- The "operational" relationship between the DVB IPTV, DVB RMS-FUS and the Broadband Forum remote management specifications (TS 102 034 [1], and TS 102 824 [2] and TR-069 [7]) is shown in clause 5 of the present document.
- The description of the RMS and FUS usage models is given in clause 6 of the present document.
- Clauses 7, 8 and 9 of the present document provide some information on the components of the solution.
- Clauses 10, 11 and 12 of the present document contain guidelines for implementation of the RMS-FUS, arranged in an order intended to reflect actual usage scenarios.
- Clause 13 of the present document contains usage guidelines for the data model components to support content download services based on the DVB Content Download Service described in TS 102 034 [1], clause 10.

Devices in the home environment are all referred to as Consumer Premises Equipment (CPEs), and this may include all IP connected devices in the home which are compliant with the DVB RMS-FUS Specification TS 102 824 [2]. This may include home network devices connected indirectly to the access network, e.g. through a router provided that IP connectivity can be arranged and that the requirements of TS 102 824 [2] are met.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

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

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

2.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 102 034 (V1.4.1): "Digital Video Broadcasting (DVB); Transport of MPEG-2 TS Based DVB Services over IP Based Networks".

[2] ETSI TS 102 824: "Digital Video Broadcasting (DVB); Remote Management and Firmware Update System for DVB IPTV Services (Phase 2)".

[3] ETSI TS 102 006 (V1.3.1): "Digital Video Broadcasting (DVB); Specification for System Software Update in DVB Systems".

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

[5] Broadband Forum TR-140: "TR-069 Data Model for Storage Service Enabled Devices", Issue Number 1.1, December 2007.

NOTE: See http://www.broadband-forum.org/technical/download/TR-140_Issue1.1.pdf.

[6] Broadband Forum TR-135: "Data Model for a TR-069 enabled STB", December 2007.

NOTE: See http://www.broadband-forum.org/technical/download/TR-135.pdf.

[7] Broadband Forum TR-069 Amendment 2: "CPE WAN Management Protocol", May 2004.

NOTE: See http://www.broadband-forum.org/technical/download/TR-069.pdf and in the context of the present document it is referred to generally as "TR-069" or "TR-069 Framework".

[8] Broadband Forum TR-106: "Data Model Template for TR-069-Enabled Devices", November 2006.

NOTE: See http://www.broadband-forum.org/technical/download/TR-106_Amendment-2.pdf.

[9] W3C Simple Object Access Protocol (SOAP) 1.1.

NOTE: See http://www.w3.org/TR/2000/NOTE-SOAP-20000508.

[10] W3C XML Schema.

NOTE: See http://www.w3.org/2001/XMLSchema.

[11] IEEE: "Organizationally Unique Identifiers (OUIs)".

NOTE: See http://standards.ieee.org/faqs/OUI.html.

[12] Void.

[13] IETF RFC 3452: "FEC - Forward Error Correction Building Block".

[14] IETF RFC 3268: "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)".

[15] IETF RFC 3926: "FLUTE - File Delivery over Unidirectional Transport".

[16] IETF RFC 4346: "The Transport Layer Security (TLS) Protocol Version 1.1".

[17] IETF RFC 2246: "The TLS Protocol, Version 1.0".

[18] IETF RFC 4217: "Securing FTP with TLS".

[19] IETF RFC 2818: "HTTP Over TLS".

[20] IETF RFC 3852: "Cryptographic Message Syntax (CMS)".

[21] Void.

[22] IETF RFC 2974: "Session Announcement Protocol".

[23] IETF RFC 4566: "SDP: Session Description Protocol".

[24] ETSI TS 102 822-2: "Broadcast and On-line Services: Search, select, and rightful use of content on personal storage systems ("TV-Anytime"); Part 2: Phase 1 - System description".

[25] ETSI TS 102 851 (V1.1.1): "Digital Video Broadcasting (DVB); Uniform Resource Identifiers (URI) for DVB Systems".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 102 542-1: "Digital Video Broadcasting (DVB); Guidelines for the implementation of DVB-IPTV Phase 1 specifications; Part 1: Core IPTV Functions".

3 Definitions and abbreviations

3.1 Definitions

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

ACS: Broadband Forum description for the server offering Remote Management functionality

NOTE: This is referred to in DVB terminology as the RMS.

boot process: sequence necessary to provision the CPE in terms of the entry IP addresses for the RMS, FUS and other DVB services

CE manufacturer: in the context of the present document this refers to the agent responsible for delivering the firmware update image file and the associated metadata to the FUS and RMS as appropriate

NOTE: In the context of the present document it may also be an alternative agency, other than the actual CE manufacturer, who supplies the firmware update and the metadata.

CPE: generic method used in the context of this present document to refer collectively to HNEDs and DNGs

delivery network: connection into the home between the delivery network gateway and the service provider

Delivery Network Gateway (DNG): device which is connected to one or multiple delivery networks and one or multiple home network segments

NOTE: See TS 102 034 [1].

DVB-IP service: DVB service provided over IP or content on demand over IP

firmware: system software of the CPE

Home Network End Device (HNED): item of equipment which is connected to a home network and which typically terminates the IP based information flow (sender or receiver side)

NOTE: See TS 102 034 [1].

Home Network End Device (HNED): device defined in TS 102 034 [1] which is connected to a home network and which typically terminates the IP based information flow (sender or receiver side)

NOTE: In the context of the present document HNEDs are included in the group of devices generally covered by the use of the term "CPE" in the present document.

managed CPE: device in the home is managed by RMS in managed network

packaging: processing of a file or object in preparation for distribution over the network

pointer announcement: information carried over the multicast service carrying redirection pointers to other locations where additional pointer, update, query, or unicast announcements are available

query announcement: information carried over the multicast service carrying redirection pointers to the location where connection can be made to the query/response channel

Remote Management System (RMS): server used for DVB Remote Management functionality

NOTE: Where BBF TR-069 methods are used this functionality is similar to the ACS in BBF terminology for the services specified by DVB.

Service Provider (SP): entity providing a service to the end-user

NOTE: In the context of the present document, SP will mean a Service Provider providing DVB-IP services.

Set Top Box (STB): method of referring to a physical device in the home, equivalent to "CPE" in the context of the present document

unicast announcement: information carried over the multicast service carrying redirection pointers to the location where connection can be made to download an update using a unicast service without any further navigation

unmanaged CPE: device in the home which is not managed by RMS or any other entities in managed network

update announcement: information carried over the multicast service carrying the descriptive information about any firmware updates which are available from the FUS

3.2 Abbreviations

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

ACS	Auto-Configuration Server
AES	Advanced Encryption Standard
B2B	Business To Business
BBF	Broadband Forum
CDS	Content Download Service
CE	Consumer Electronics
CPE	Customer Premises Equipment
CWMP	CPE Wan Management Protocol
DHCP	Dynamic Host Configuration Protocol
DNG	Delivery Network Gateway
DSM-CC	Digital Storage Media - Command and Control
DVB	Digital Video Broadcasting
DVBSTP	DVB SD&S Transport Protocol
FTP	File Transfer Protocol
FUS	Firmware Update System
FUSS	FUS stub file
HNED	Home Network End Device
HTTP	Hyper Text Transfer Protocol
ID	IDentifier
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPI	Internet Protocol Infrastructure
IPv4	Internet Protocol version 4
MAC	Media Access Control, depending on context
NTP	Network Time Protocol
QRC	Query/response channel
RFC	Request For Comments
RMS	Remote Management System
RPC	Remote Procedure Call
SAP	Service Announcement Protocol
SD&S	Service Discovery and Selection
SDP	Service Description Protocol

SFTP	SSH File transfer Protocol
SOAP	Simple Object Access Protocol
SP	Service Provider
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TFTP	Trivial Filr transfer Protocol
TLS	Transaction Layer Security
UDP	User Datagram Protocol
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WWW	World Wide Web
XML	eXtensible Markup Language

4 System Reference Model

The logical architecture is shown in figure 1 which is copied from TS 102 824 [2], clause 5. Table 1 of TS 102 824 [2] is also copied below (for information) and gives an introduction to the interfaces used in the architecture with a description of their function and whether they are specified in TS 102 824 [2] or assumed to be out of scope, for example, of a business-to-business (B2B) type.

The RMS and FUS are shown as logically separate since although TS 102 824 [2] describes the operation and features which can be supported in combination, it also describes usage models for managed and unmanaged CPEs where in each case only some parts of the system is needed.

For the unmanaged CPE usage model it is assumed that there is no RMS, and that the CPE identifies the location of the appropriate update file either at boot time from the FUSS or using the announcement methods (multicast and/or unicast) defined in TS 102 824 [2].

For the managed CPE there are two usage models enabled in TS 102 824 [2].

For the RMS-only (managed) usage model firmware update is not supported using the methods described in TS 102 824 [2], and only the RMS is required. The method of managing and delivering the actual download file is considered to be out of scope. In this case the extended capabilities which DVB have added to those defined in the Broadband Forum TR-069 [7] may be used over the management channel.

For the RMS-FUS usage model it is assumed that the RMS controls the FUS for managed CPEs. The methods for the communication between the CPE and RMS across the access network are defined in the appropriate remote management specification, e.g. Broadband Forum TR-069, but the behaviour associated with the firmware update is defined in TS 102 034 [1]. After boot time the CPE uses the RMS management channel to identify the location of the appropriate update file, and the update delivery is from the FUS. Use of the FUS announcement services (multicast and/or unicast) is not but may be used as part of the CPE/RMS behavioural model. Alternatively, message types have been added to the original Broadband Forum management vocabulary defined in TR-069 [7] to allow reporting back by a managed CPE to the RMS after the CPE has autonomously carried out an update based on the FUS announcement messages. At boot time a managed CPE may be informed of the location of an appropriate update file by the FUSS file, or directly by the RMS over the management channel (interface 9) after bootup and IP provisioning, described in TS 102 034 [1].

A single FUS may be used to support one or both of these modes for different CPE population groups. Tables 2 and 3 define which interfaces (messaging, announcements and delivery) are required for each of the modes for the server (RMS and FUS) and client (CPE) devices.

An RMS may use multiple FUSs to serve updates to a supported population of managed CPEs.

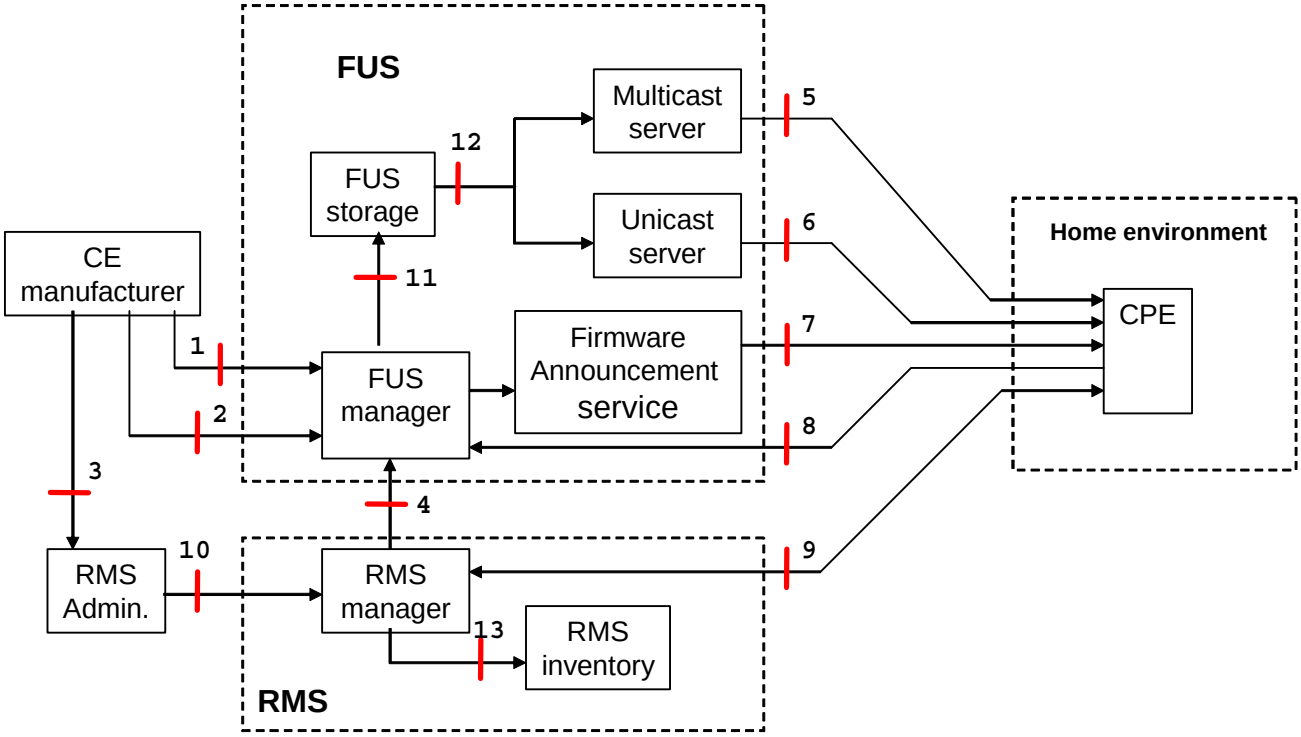


Figure 1: DVB RMS-FUS Logical Architecture

Table 1: Overview of interface functions

Interface number	Interface name	Description	Scope in terms of the present document
1	Firmware package	This carries the files containing the firmware from the CE manufacturer to the FUS will be carried on this interface if the standardised mechanism is used.	Out of scope.
2	Metadata	Metadata provided by the CE manufacturer to describe the properties of the firmware update package for the RMS and FUS.	Schema Definition (XML) standardised, use across this interface is recommended.
3	CE manufacturer - RMS administrator	B2B relationship between CE manufacturer and RMS administration.	Schema Definition (XML) standardised, use across this interface is recommended.
4	RMS-FUS control interface	Metadata passed from FUS to RMS and RMS to FUS to manage the download behaviour.	Schema Definition (XML) standardised, use across this interface is recommended.
5	Multicast delivery	Multicast delivery as a service over the network to the population of CPEs.	Transport protocol options standardised. Authentication of source recommended, method not specified. Payload protection is not standardised. Refer to clause 6.5 for detail.
6	Unicast delivery	Unicast delivery as a service over the network to the population of CPEs.	Transport protocol options standardised. Authentication of source and destination recommended, method not specified. Payload protection is not standardised. Refer to clause 6.6 for detail.
7	Firmware announcement interface	This service carries notification information about firmware updates which are available over the network.	Schema Definition (XML) standardised Transport protocol options standardised Authentication of source recommended, method not specified. Payload protection is not standardised. Refer to clause 6.7 for detail.
8	Query Response Channel (QRC)	In the FUS-only model this enables the CPE to query the FUS to find out if firmware updates are available for CPE.	Transport protocol and RPC arguments standardised. Authentication of source and destination recommended, method not specified. Refer to clause 6.8 for detail.

Interface number	Interface name	Description	Scope in terms of the present document
9	CPE management	This interface may be compliant with BBF TR-069 with DVB specified extensions (recommended solution) or other functionally equivalent protocols such as Cable Labs PACM with extensions (not specified in the present document).	Profile and extensions to TR-069 [7] specified by DVB in cooperation with BBF. Refer to clause 6.9 for detail.
10	RMS administration	B2B interface between RMS administrator and RMS.	Out of scope.
11	FUS storage	Internal to FUS.	Out of scope.
12	FUS processing	Internal to FUS.	Out of scope.
13	RMS inventory	Internal to RMS.	Out of scope.

For the server (FUS/RMS) and CPE each row of tables 2 and 3 shows the possible combination of interfaces. Additional features over and above those combinations required for conformance optionally some offer additional functionality to the RMS-FUS system.

NOTE: These tables are reproduced here from TS 102 824 [2], but the definitive version should be taken from that specification document.

Table 2: Interface conformance - server side

Server side requirements							
	Interfaces					Conformance to DVB RMS-FUS specification	Comments
	5	6	7	8	9		
RMS-FUS	X	X		X	X	Not conformant	Interface 7 is required for the multicast announcement.
	X	X	X	X	X	Optional	Full implementation is optional.
	X	X	X		X	Required	Interface 9 is required to be able to replace all functionalities of interface 8.
FUS-only	X	X		X		Not conformant	Interface 7 is required for the multicast announcement.

Table 3: Interface conformance - CPE side

CPEs requirements							
	Interfaces						
	5	6	7	8	9		
Managed	X		X		X	Optional	Only one of these interfaces combinations must be supported by the managed CPE.
	X	X	X	X	X	Optional	
		X		X	X	Optional	
		X			X	Optional	
	X	X	X		X	Optional	
Unmanaged	X		X			Optional	Only one of these interfaces combinations must be supported by the unmanaged CPE.
		X		X		Optional	
	X	X	X	X		Optional	

5 Usage models

5.1 Remote management only

Remote management only is intended as a method for DVB home devices (CPEs) to be managed by a Service Provider or designated third parties where DVB firmware update is not used.

The remote management interface is specified in accordance with the Broadband Forum TR-069 [7] methods but alternatives may be used, e.g. the method specified by Cablelabs, but the additional interfaces, e.g. additional RPCs, and parameters for these alternatives are not specified in TS 102 824 [2]. In cases where the Broadband Forum methods are used the boot process will provide the location of the RMS server which the CPE can use for the initial connection to using an INFORM message.

Annex A (clauses A.1 and A.2) of the RMS-FUS specification (TS 102 824 [2]) provides a brief description of the CWMP (TR-069) protocol RPCs (Remote Procedure Calls) that need to be used for Firmware Update. The DVB RMS-FUS specification does not mandate the level of management to be applied by the Service Provider, or restrict the Service Provider from extending the specification using the vendor specific fields included in TR-069 [7].

No multicast methods are supported in this model and only HTTP(S) is assumed as the protocol for messaging.

Authentication of server and client for any relationship may be required using the methods described in the specification, and in the case of a security breach methods of recovering the security are possible within this model.

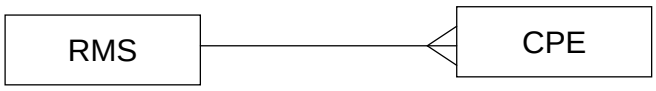


Figure 2: Relationship between RMS-FUS devices for RMS-only functionality

TR-069 [7] includes support for both unicast and multicast download of firmware updates, based on the methods defined in TS 102 824 [2], which extended previous methods of the TR-069 specification [7].

Any single CPE can only be managed by a single RMS at any instant in time, but management of a CPE may be transferred over to another RMS when necessary.

5.2 Firmware Update only

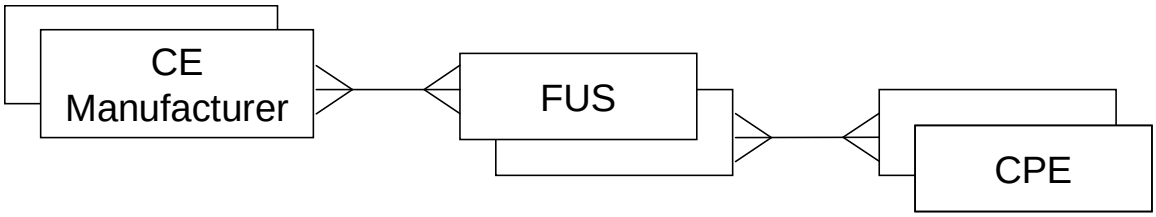


Figure 3: Relationship between RMS-FUS devices for FUS-only functionality

The full description of the functionality of the FUS is given in TS 102 824 [2], clause 5.3.

This model is defined in order to allow CE manufacturers to download firmware updates to unmanaged CPEs without the need for any RMS. In the absence of the RMS the management interface is not available.

The firmware update files will be downloaded from the CE manufacturers to the FUS, with the descriptive metadata. The FUS must be able to prepare the update files for delivery to the CPEs and expose it available either in a unicast (query-response) or multicast (carousel) service to the CPE. Protection (authentication, etc.) of the actual firmware update payload file contents is not specified in TS 102 824 [2], it is assumed that the agencies involved will arrange that protection in a way agnostic to the delivery.

The FUS will process the update files into a form that can be carried over either multicast, unicast or both in the payload format appropriate for that CPE. The relevant information describing the delivery of those downloads will be added to the metadata from the CE manufacturer to be used to create the multicast announcement messages carried over interface 7 (see figure 1) enabling the FUS to respond to queries from the CPE on the unicast interface 8. The metadata is described in clause 7.

If a firmware update exists for any specific CPE of group of CPEs there will be a specific instance of metadata providing all the information to make a connection to the server and download the firmware update. There may be more than one multicast announcement service and more than one unicast query address available from the FUS for different populations of CPEs and different CE manufacturers.

Authentication of server and client for any relationship can be performed using certificates embedded in the CPE firmware using the methods described in the FUS specification, but without an RMS or additional secure channel updates to the security (data authentication, integrity and consistency) cannot be done within this model.

Unmanaged CPEs may be updated to become managed if a user makes a contract with a Service Provider or third party management organisation whose services are allowed through the network.

5.3 Combined RMS/FUS implementations

This again follows the BBF TR-069 [7] methods with the additional functionality described in annex A of TS 102 824 [2] for DVB home devices.

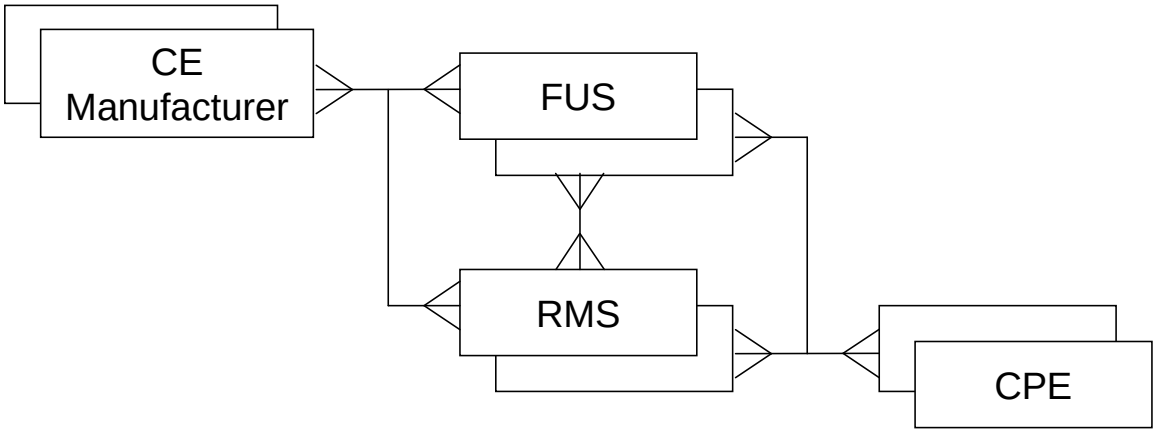


Figure 4: Relationship between RMS-FUS devices for combination RMS-FUS functionality

This is a combination of the remote management and the firmware update processes in which both usage models described above are available as operation modes that exploit only part of the available functionalities. An additional one is also available, fully exploiting the functionalities of the system, in which the RMS configures the CPE(s) with the information needed to contact the FUS server and autonomously carry out the Firmware Update. The CPE(s), after carrying out the Firmware Update, notifies back the RMS about the completion status of the process. To do this the CWMP extensions described in annex A of TS 102 824 [2] are needed.

For any single CPE the RMS management channel operates for remote management purposes in a similar way to the RMS-only case described in clause 5.2.1 with a single RMS managing a managed CPE at any instance in time. A single RMS may use multiple FUSs to serve the population of CPEs under its control.

6 Relationship between IPTV Handbook, DVB RMS-FUS specification and the Broadband Forum Remote Management framework specification

The documents referred to are:

- The DVB IPTV handbook, published as TS 102 034 with the first version which is relevant to the RMS-FUS Specification being revision 1.4 [1].
- The DVB RMS-FUS Specification, TS 102 824 [2].
- The Broadband Forum framework specification is TR-069 [7].

The "operational" relationships between TS 102 034 [1] (revision 1.4 of the DVB IPTV Handbook), TS 102 824 [2] (DVB RMS-FUS specification) and TR-069 [7] (the BBF Remote Management specification) are illustrated in the following series of diagrams for the different scenarios. Dashed lines indicate alternative options.

For the scenarios starting from bootup (1), the first operation is to look for the FUSS (FUS Stub file) if it exists (2) using one of the methods described in clause 9.1 of TS 102 034 [1]. In the absence of a FUSS file the process would proceed to the acquisition of the IPTV provisioning information (3) such as the SD&S location, and the location of any appropriate update file must then be obtained using the methods described in clause 5 of TS 102 034 [1]. Operation (4) indicates the start of the CPE in its normal operating mode.

For the RMS-only scenario in a DVB IP environment it is assumed that the RMS location will either be hard-coded in the CPE or be obtained from the SD&S. Methods specific to the RMS, e.g. based on DHCP options at boot, can be made available by other standards such as TR-069 [7].

6.1 Managed CPEs using RMS-only for startup and during normal operation

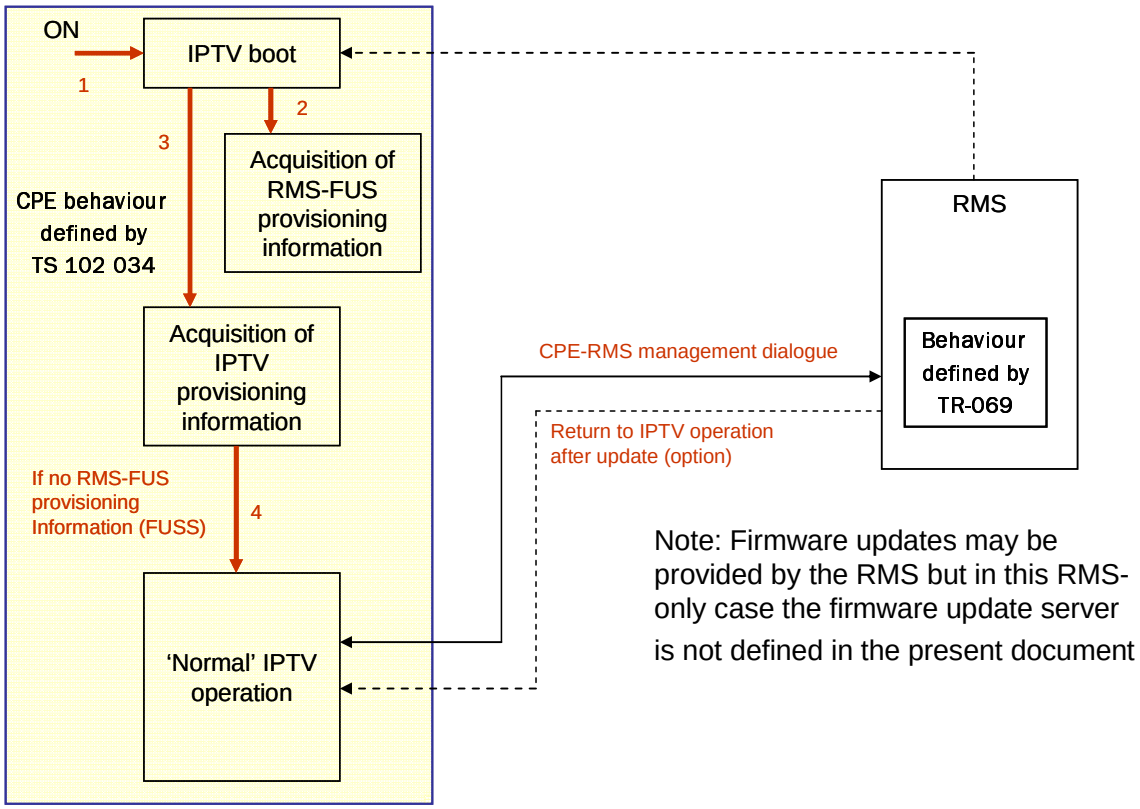


Figure 5: Relationship between standards for RMS-only use case - Startup and normal operation

This scenario assumes that the RMS location is already known by the CPE or can be obtained from the SD&S RMS-FUS record and that the complete sequence would be controlled by messaging over interface 9.

At startup a typical operational flow would be that the management process would be initiated by the CPE with an "INFORM" message to the RMS to announce that it is active and connected. If there is an update the RMS will deliver the URL where the update is located. The update will be delivered from the URL provided and the 'TRANSFERCOMPLETE' message is returned to the RMS. The detail of the download server is out of scope of TS 102 824 [2] and no association with the DVB RMS-FUS specification TS 102 824 [2] is necessary.

During normal operation, the interaction is between the CPE and RMS and may be initiated by either device, the functionality is described in TR-069 [7], profiled by the additions or restrictions specified in TS 102 824 [2]. In this case step 1 could be a periodic check by the CPE to the RMS to see if any updates are available, if there are none the return will be immediate. Another option could be the RMS that sends a ConnectionRequest to the CPE to start a management session when a new firmware is available. If there is a suitable update the RMS will deliver the URL where the update is located. The update will be delivered based on the URL provided (2) and the process usually ends with the 'TRANSFERCOMPLETE' message returned to the RMS. In the diagram above the download server is assumed to be part of the RMS, though this may not be true.

6.2 Managed CPEs using RMS-FUS for startup and during normal operation

Both startup and normal operation processes can be described by figure 6, it is assumed that the location of the RMS is known to the CPE either through one of the provisioning mechanisms at boot, from the SD&S record or by hardcoding in the CPE, and that no FUSS file is available for that CPE. The remote management dialogue can therefore be considered to start after the initial IPTV bootup and provisioning.

The complete sequence would be controlled by CPE-RMS messaging over interface 9 and RMS-FUS messaging over interface 4.

As an example, at startup the CPE would initiate the interaction with an "INFORM" message to the RMS to announce that it is active and connected. If there is an update the RMS will deliver the URL where the update is located. The update will be delivered from the URL provided and the 'TRANSFERCOMPLETE' message is returned to the RMS. The detail of the download server, the FUS, is defined in TS 102 824 [2] and the methods defined in TS 102 824 [2] by DVB as extensions to the BBF TR-069 [7] methods may be used.

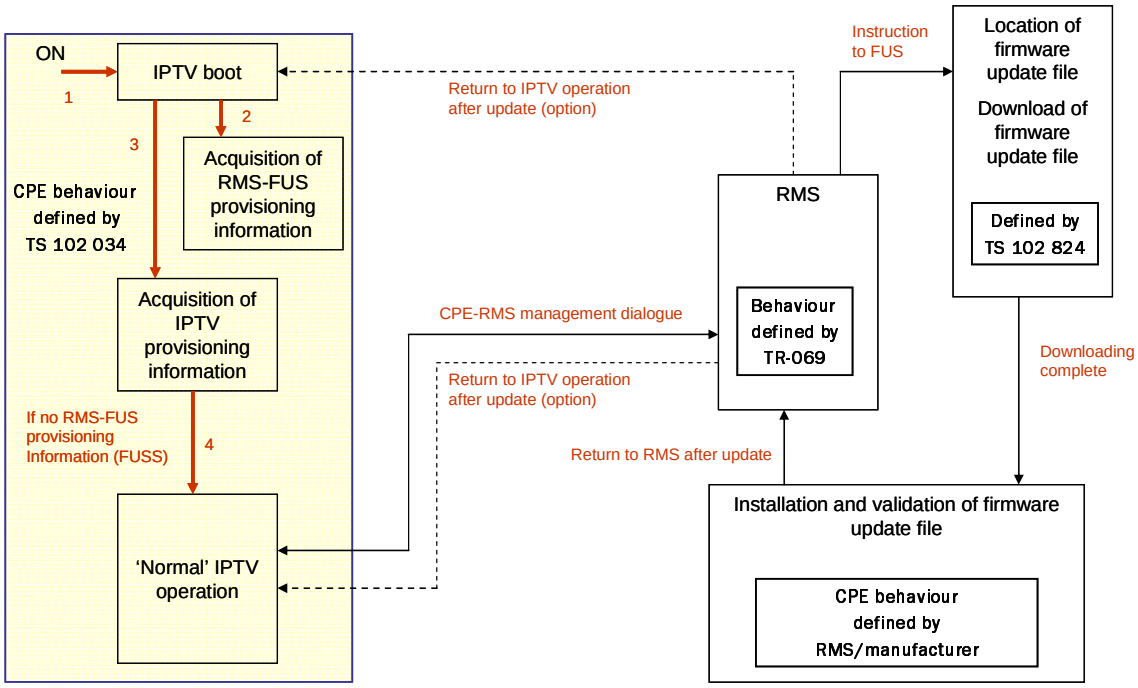


Figure 6: Relationship between standards for RMS-FUS use case - Startup and normal operation

During normal operation, the interaction between the CPE and RMS may be initiated by either device, the CPE-RMS management functionality is described in TR-069 [7], profiled by the additions or restrictions specified in TS 102 824 [2]. In this case a periodic check by the CPE to the RMS to see if any updates are available may be used, if there are none the return will be immediate. If there is a suitable update the RMS will deliver the URL where the update is located through a DOWNLOAD RPC. The update will be delivered based on the URL provided (2) and when the download is over the 'TRANSFERCOMPLETE' message is usually returned to the RMS.

In both cases the return after an update may either be via a reboot or more directly to the normal operation mode.

6.3 Unmanaged CPEs using FUS-only for startup operation

At startup the first action will be for the CPE to look for an FUSS file containing an appropriate firmware update location, and if one exists the CPE can use this location to make a connection to the FUS to download and install the updated image file. If there is no FUSS file the remainder of the boot and provisioning procedure should be carried out and the process for locating an update would be similar to that described for normal operation.

During normal operation the multicast and unicast announcement services as advertised in the SD&S may be used to obtain the location of an update. The update file would be downloaded and installed in the CPE.

In both cases the CPE may report to the manufacturer or to a 3rd party whether the update was successful using an address provided in the announcement metadata, and the return after an update may either be via a reboot or more directly to the normal operation mode depending on the programmed behaviour of the CPE and the type of update carried out.

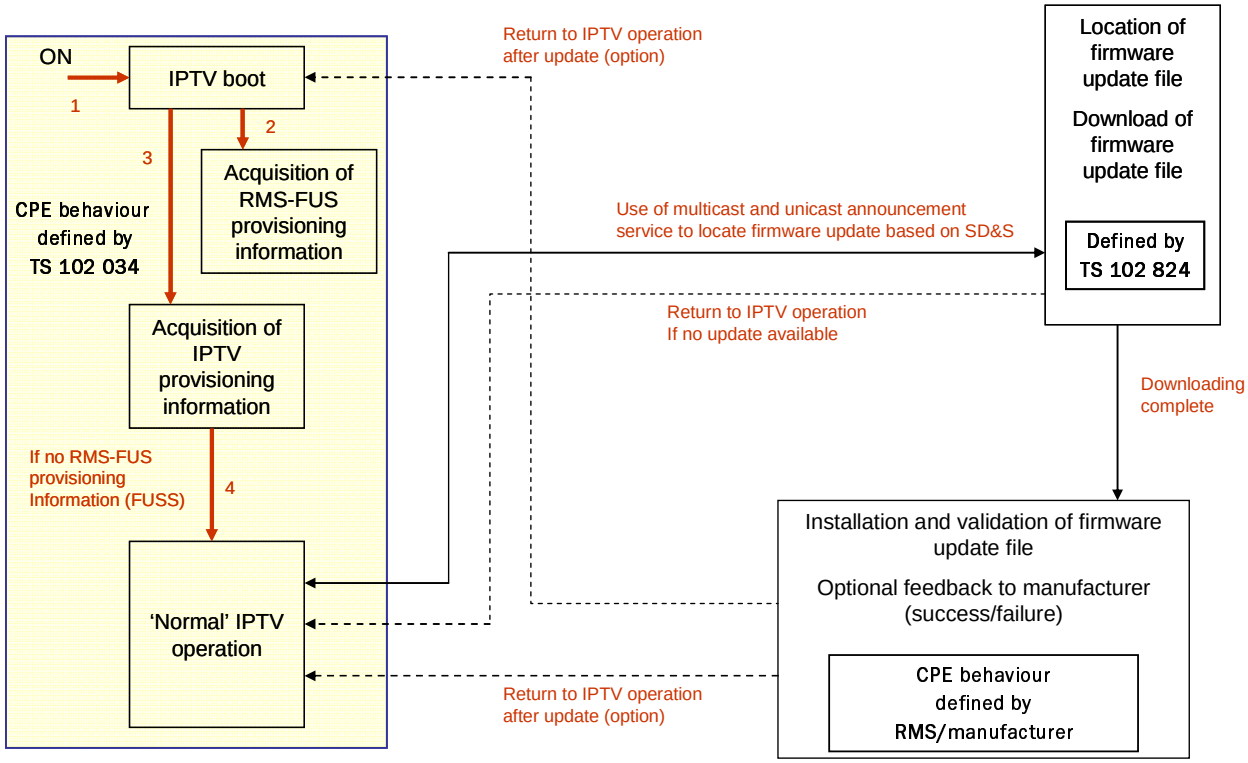


Figure 7: Relationship between standards for FUS-only use case - Startup operation

7 RMS-FUS metadata

The schema uses the "w3c.org" base and is defined as "ipi-rms:phase2:2009-01" using elements and attributes specified within the RMS-FUS Task Force specifically for the schema.

All character encoding is in UTF-8. All Types specified by w3c use the "xsd" namespace, and those defined within the DVB RMS-FUS Task Force use "rms" namespace.

7.1 Overview

An XML metadata structure defines the properties of the firmware files based on information from all the entities which contribute to the creation, announcement and distribution, downloading and reporting. A textual version of the metadata is shown for information in annex B, the definitive version is in the schema (defined as "ipi-rms:phase2:2009-01") provided with the DVB RMS-FUS Specification.

Each XML instance based on the schema will describe a particular firmware update file and indicate the CPE targeting for that file.

The schema overview is shown in figures 8 and 9. Figure 8 gives a listing of the local type definitions used throughout the schema definition, The type definitions include simple element definitions and also groupings of the simple element definitions which are appropriate as hierarchical components for the overall schema. The schema definition is the final item and figure 9 shows the structure of the description part of the schema built on these locally defined types.

Where appropriate, these element groupings are directly aligned with those used by Broadband Forum and specified in the TR-069 family of documents.

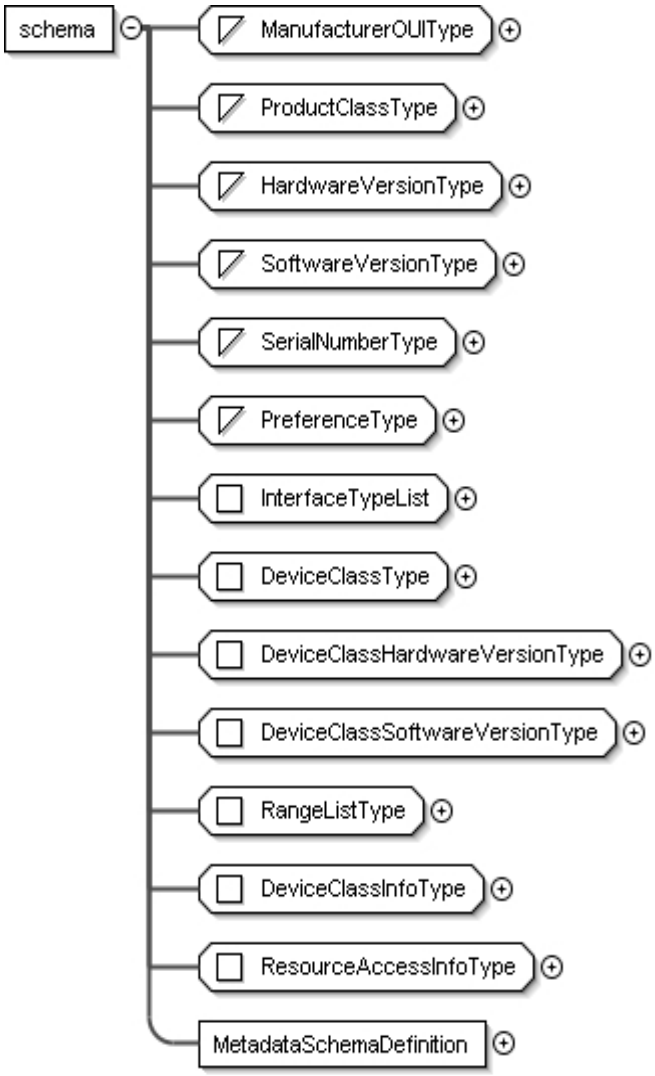


Figure 8: View of total schema structure

The schema structure represents a reference point for the aggregation of all the information about a single download file, although not all parts of the description are appropriate to all the entities in the chain from the CE Manufacture to the CPE. Information will be provided by the appropriate entity to describe their part of the system and to allow the other entities to carry out the tasks needed to update the firmware of a CPE. It is assumed that there might be some shared methods between the CE Manufacture, the RMS and the CPE in terms of payload security.

The main parts of the metadata schema from the overview above are introduced in the clauses following, the element groups are then described and the more detailed description of each entity group completes this description.

All the message structures used for SDP (as defined in RFC 4566 [23] or query-response announcements and queries use elements groups based on this schema.

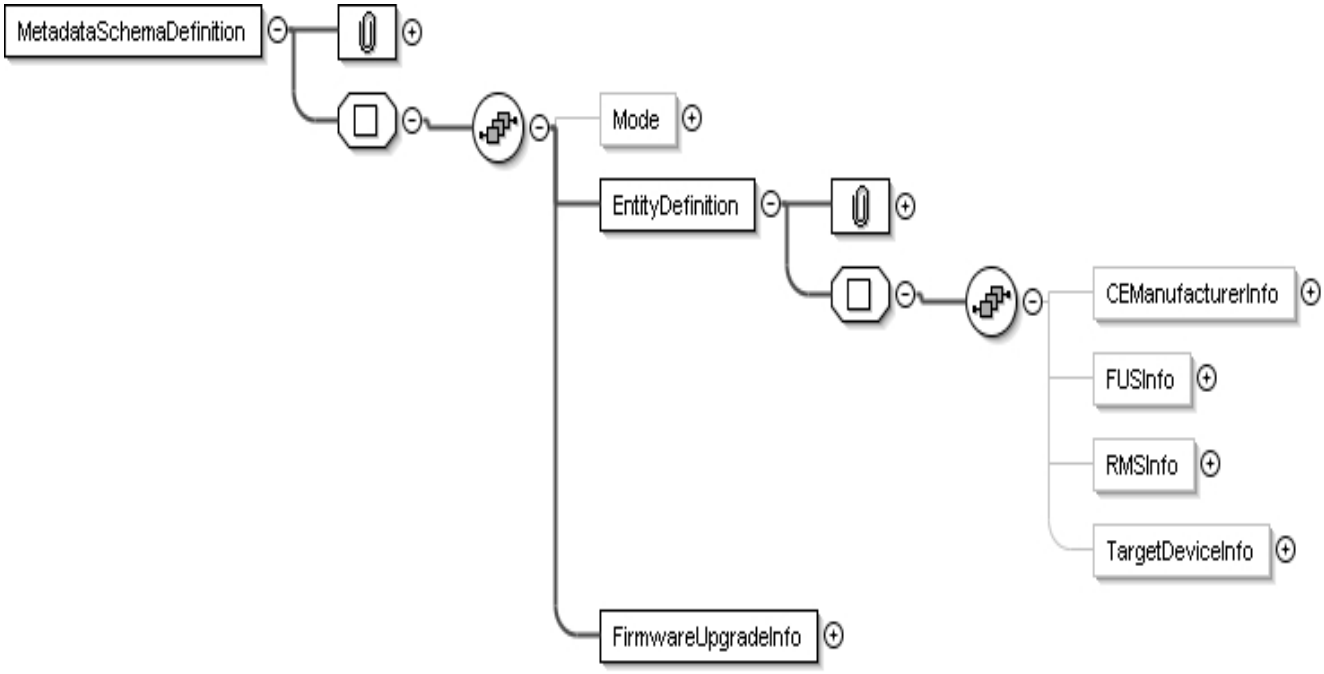


Figure 9: Overview of Metadata schema structure

7.2 Definition of locally defined types

The simple Types defined in this clause will be used either as described or in groups to from the complex Types defined in the present document. These will be used throughout the main schema definition. These Types will carry the "rms" namespace in the schema definition.

7.2.1 ManufacturerOUIType

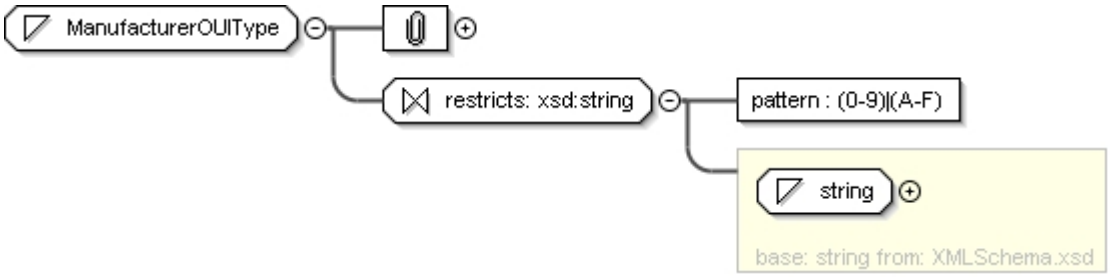


Figure 10: Manufacturer OUI container

The manufacturer OUI uniquely identifies the manufacturer and is a 6 digit hexadecimal number conformant with the IEEE OUI specification [11].

7.2.2 ProductClassType

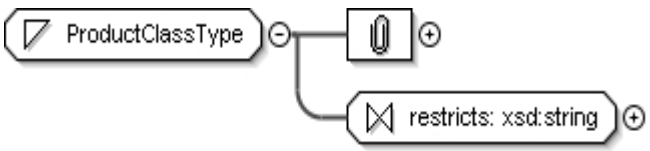


Figure 11: Product class container

The product class is a string defined by the manufacturer to describe the CPE entity within the manufacturer's range. No specific constraints are applied to this field beyond those which normally apply in an XML document. This is used to establish compatibility for available firmware updates.

7.2.3 HardwareVersionType

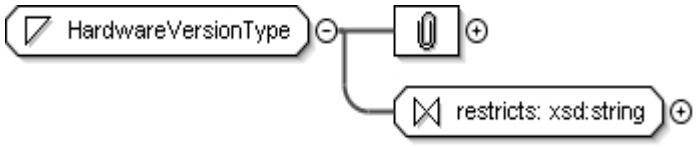


Figure 12: Hardware version container

The hardware version is a string defined by the manufacturer to describe the hardware platform of the CPE within the manufacturer's range. No specific constraints are applied to this field. This is used to establish compatibility for available firmware updates.

7.2.4 SoftwareVersionType

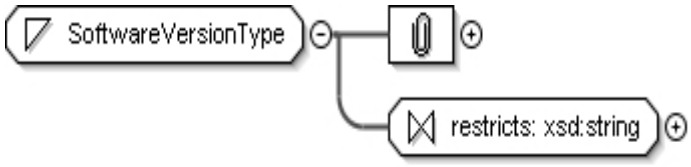


Figure 13: Software version container

The software version is a string defined by the manufacturer to describe the current software platform of the CPE within the manufacturer's range. No specific constraints are applied to this field. This is used to establish compatibility for available firmware updates.

7.2.5 SerialNumberType

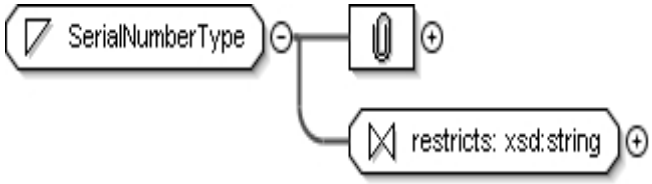


Figure 14: Serial number container

The serial number is normally considered to be specific to each instance of a CPE, it is carried as a string with no specific constraints in this field. It can be used as a component of a list of one or more serial numbers or as the start and finish values for a range of serial numbers to be targeted (see RangeListType following) in a firmware update operation. This may be done for reasons such as software beta testing, or to minimise the risk of corrupting a complete population of similar CPEs by sending an update to the whole population together.

7.2.6 RangeListType

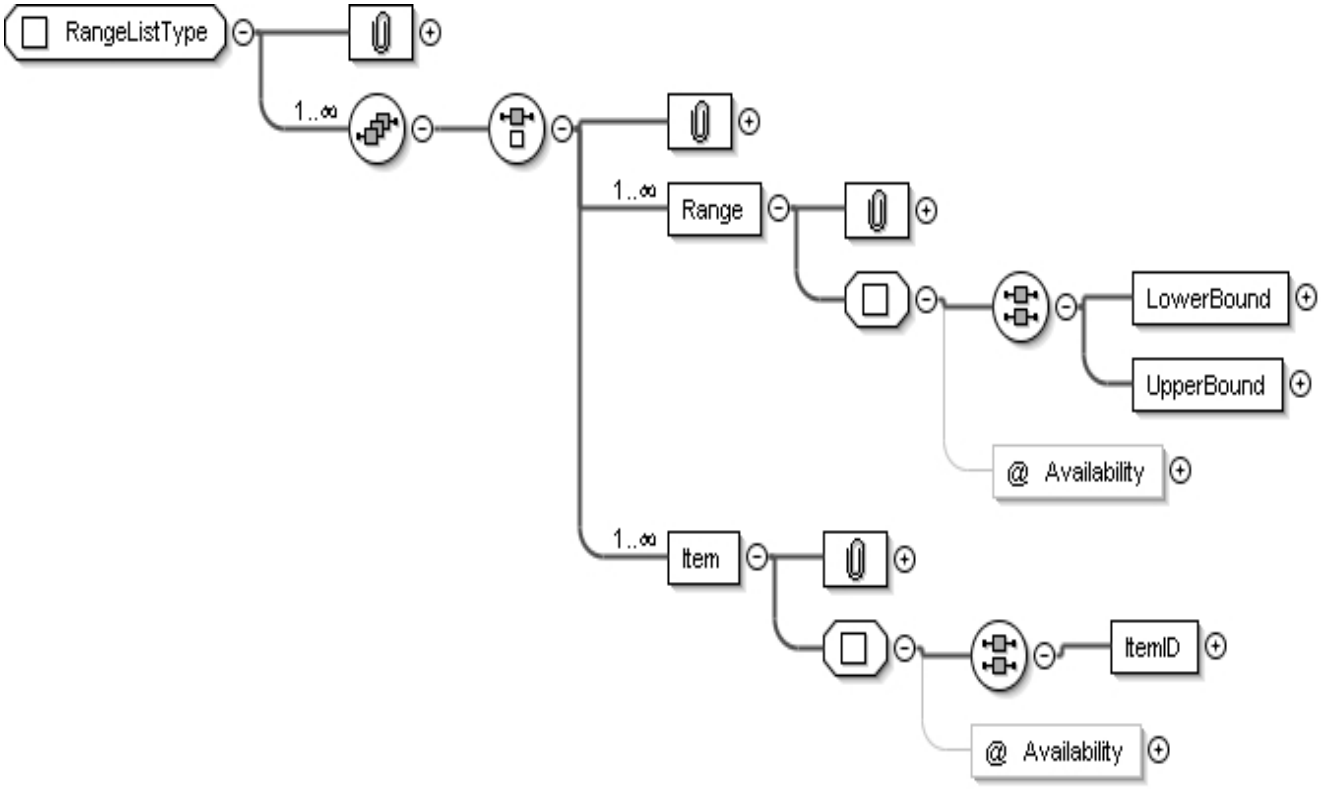


Figure 15: RangeListType definition

In order to provide a unique description of one or more CPEs, fixed properties such as serial number and MAC address can be used. All elements are in the form of unconstrained strings. This structure defines how groupings of serial numbers and/or MAC addresses can identify:

- Contiguous ranges of identifiers using the "Range.LowerBound" and "Range.UpperBound" fields.
- Non-contiguous lists of identifiers using multiple instances of the "Item" field.ItemID.

In each case the "Availability" attribute can indicate inclusion or exclusion to minimise the number of identifiers which must be advertised.

Range may be used multiple times within a single XML instance to include multiple lists, each of which is contiguous, and in combination with lists of non-contiguous items. Where multiple Ranges or Items are used the combinations of ranges or lists must be functionally be considered as a logical "AND". The example below shows a combination of target serial numbers from 123123 - 456456, excluding 231231 - 255555, and including 678678, 678688, 678698 and 678778.

```
…
<RangeList>
    <Range>@Inclusive
        <LowerBound>123123</LowerBound>
        <UpperBound>456456</UpperBound>
    </range>
    <Range>@Exclusive
        <LowerBound>231231</LowerBound>
        <UpperBound>255555</UpperBound>
    </range>
    <Item>@ Inclusive
        <ItemID>678678</ItemID>
        <ItemID>678688</ItemID>
        <ItemID>678698</ItemID>
        <ItemID>678778</ItemID>
    </Item>
</RangeList>
…
```

7.2.7 PreferenceType

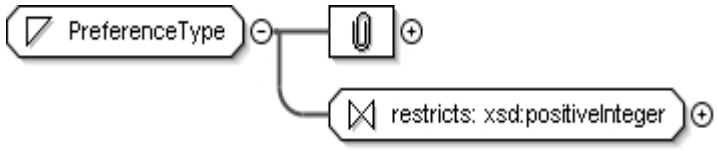


Figure 16: Preference container

For some fields in the schema multiple options may be offered with a preferred ordering, this PreferenceType is used to support those cases. It is in the form of a positive integer for which the lowest value has highest priority.

7.2.8 InterfaceType

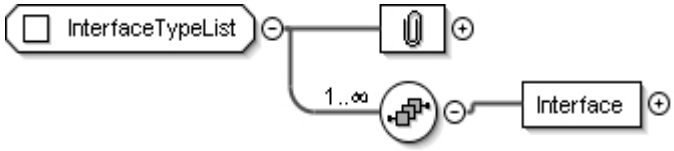


Figure 17: Interface container

This is the generic interface definition field specified for RMS-FUS listing a list of all the external (referenced to the architecture model, figure 1 in TS 102 824 [2]). The fields are strings constrained to the values as below:

1) Firmware Package;
2) Metadata;
3) RMS Administrator;
4) FUS Interface;
5) Multicast Delivery;
6) Unicast Delivery;
7) Firmware Announcement;
8) Query Response Channel;
9) CPE Management.

7.2.9 DeviceClassType

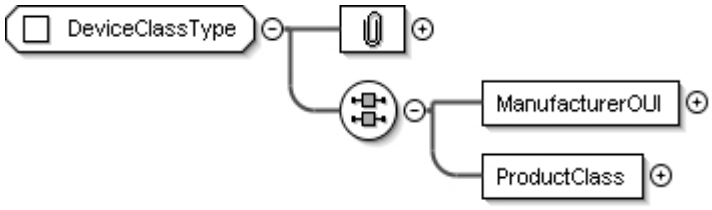


Figure 18: Device class container

The DeviceClassType defines the information structure needed to define a specific type of product specific to a manufacture.

7.2.10 DeviceClassHardwareVersionType

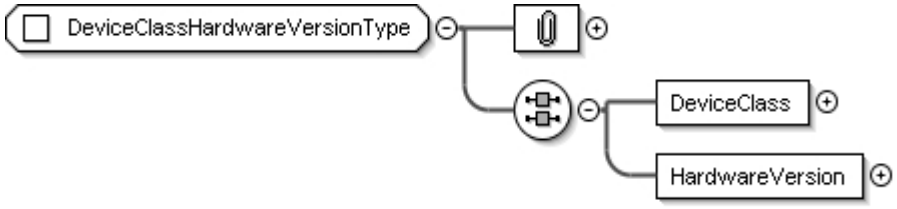


Figure 19: Device class and hardware container

This grouping extends the DeviceClassType to provide more complete CPE targeting information also based on the hardware version.

7.2.11 DeviceClassSoftwareType

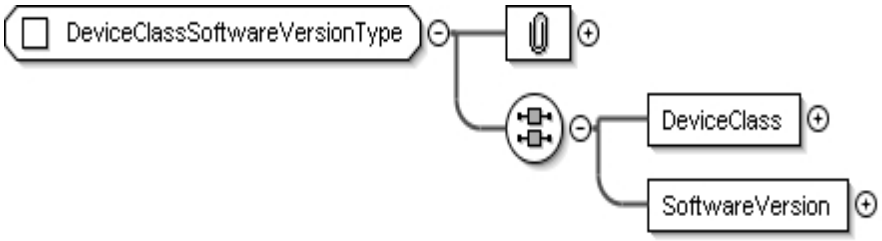


Figure 20: Device class and software container

This grouping extends the DeviceClassType to provide more complete CPE targeting information also based on the software version.

7.2.12 DeviceClassInfoType

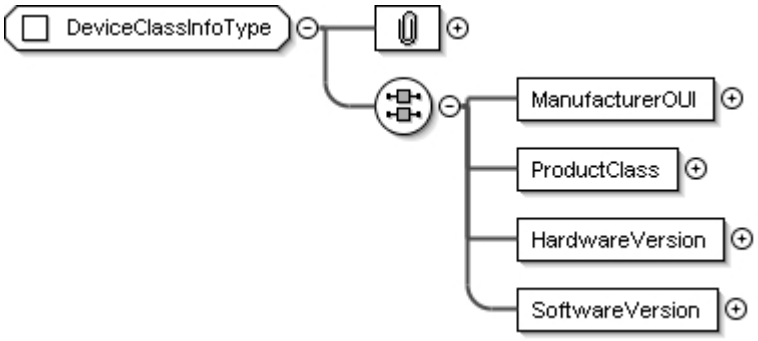


Figure 21: Device class information container

The DeviceClass Info Type defines a grouping containing the whole population of a more tightly specified group based on manufacturer, product class, and hardware and software versions.

7.2.13 ResourceAccessInfoType

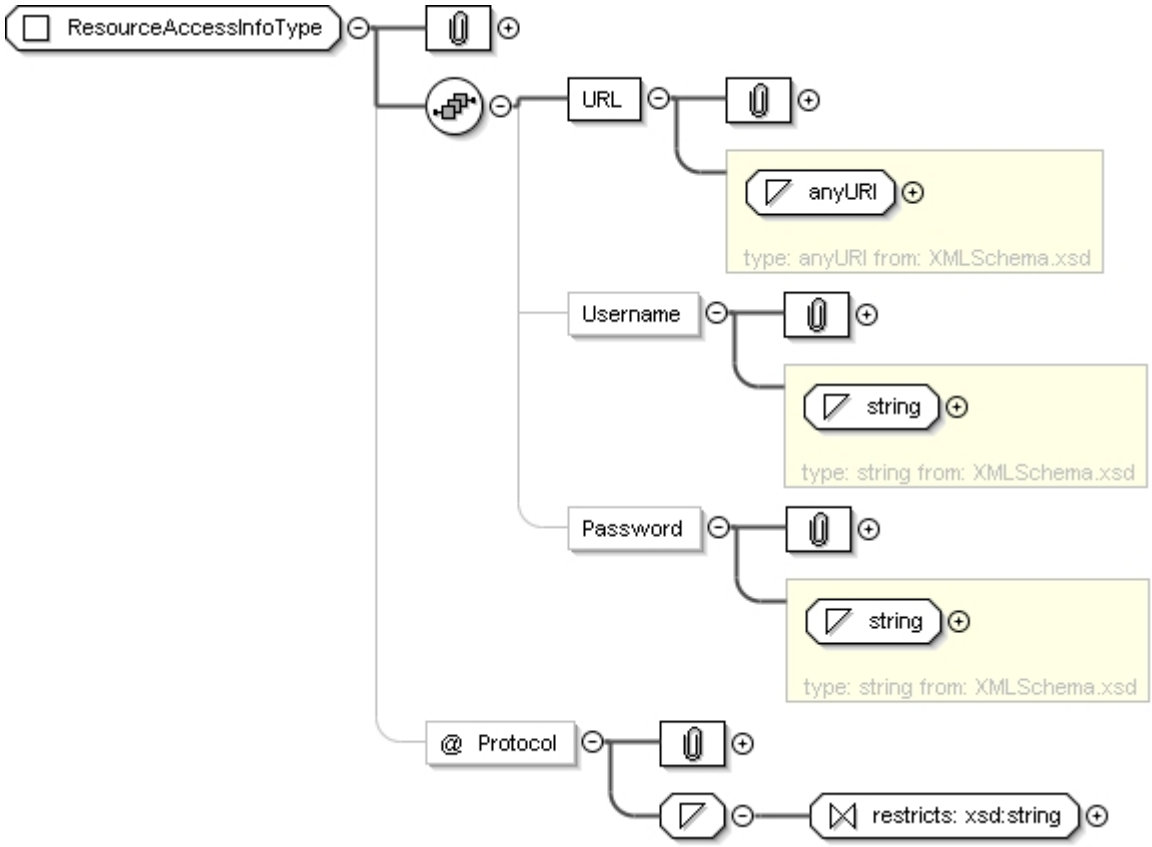


Figure 22: Resource access information container

The ResourceAccessInfoType defines a generic structure to be used in definitions of interfaces. The generic structure and optional status of the elements within it allow an adaptable description of any interface or connection used in the DVB RMS-FUS specification to be included.

The profiling of this Type is described in TS 102 824 [2] for each example of its usage.

7.3 Locally defined element sub-structures and groupings

These are based on the type definitions above but are used in the main descriptive schemas, they are described in this separate clause in order to clarify presentation.

7.3.1 DeviceGroup

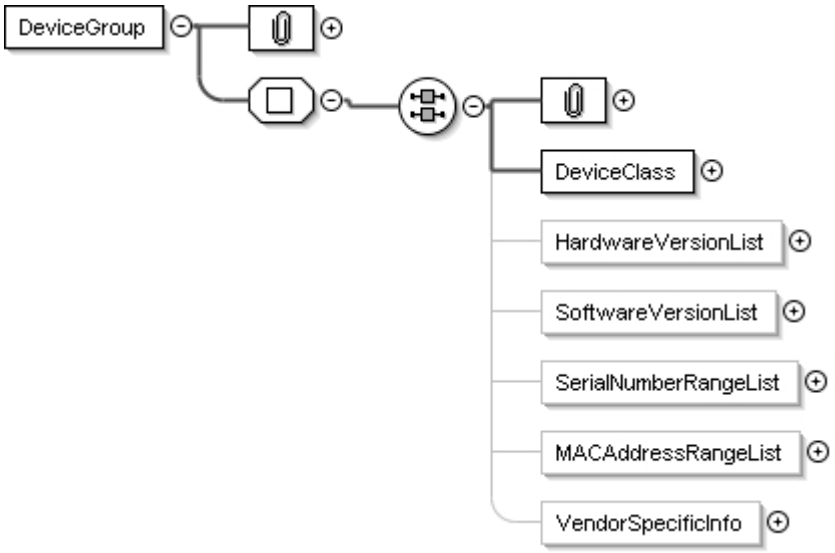


Figure 23: Device group container

This contains the following element grouping which should be combined as an 'AND' function:

- DeviceClass - this Type is defined in clause 7.2.9, it includes ManufacturerOUI and ProductClass.
- HardwareVersionList - this container element is locally defined to carry one or more hardware platform versions (HardwareVersionType defined in clause 7.2.3) for which the software update is appropriate, each instance of this data shall be formatted as a 'string'.
- SoftwareVersionList - this container element is locally defined to carry one or more software versions (SoftwareVersionType defined in clause 7.2.4) which can be directly replaced by the update, each instance of this data shall be formatted as a 'string'.
- SerialNumberRangeList - one or more ranges or a list (inclusive or exclusive) of CPE serial numbers for which the update should apply, this is based on the RangeListType defined in clause 7.2.6. An example is shown in clause 7.2.6.
- MACAddressRangeList - one or more ranges or a list (inclusive or exclusive) of CPE MAC addresses (assumed to be 'fixed' for a CPE) for which the update should apply, this is based on the RangeListType defined in clause 7.2.6. An example based on serial numbers is shown in clause 7.2.6.
- VendorSpecificInfo - any additional information specific to the update, no specific format is specified for this element.

The combination allows flexible but precise targeting of firmware updates to specific populations of CPEs.

An example is:

```
…
<FirmwareUpgradeInfo>
    <Software Version>
        <DeviceClass>
<ManufacturerOUI>A123DF</ManufacturerOUI>
<ProductClass>STB-04100r2</ ProductClass>
        </DeviceClass>
    </Software Version>
    ...
</FirmwareUpgradeInfo>
…
```

7.3.2 SoftwarePackageInfo

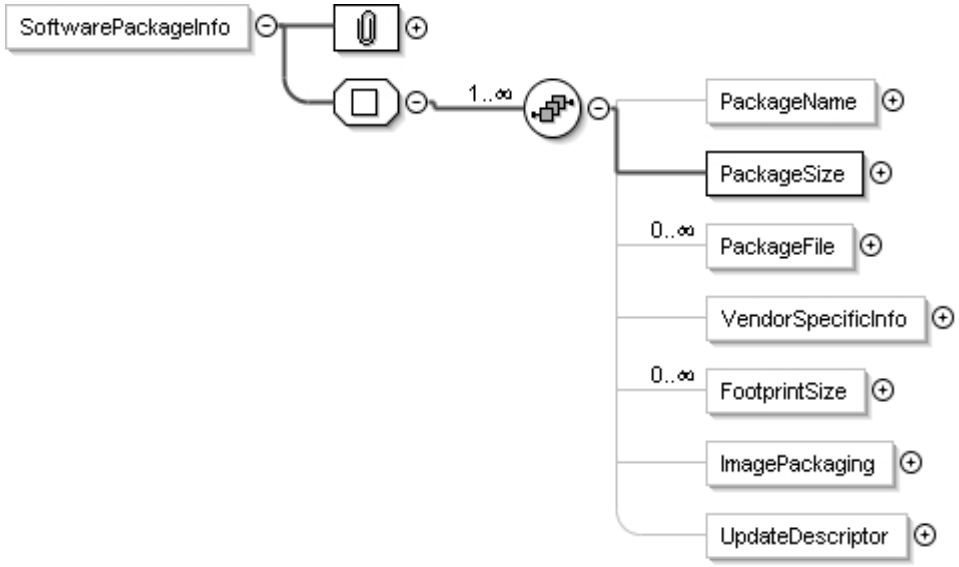


Figure 24: Software package information container

A firmware update package delivery may contain multiple files of different types. This grouping specifically describes the firmware update package structure of that information and is made up of:

- PackageName - the name of the update package, this string may only be intended to be 'machine-readable'.
- PackageSize - the (integer) size of the update package in bytes.
- PackageFile - an optional sub-structure containing multiple descriptions of files used to complete the update, for each file the information is as follows:
  - FileName - the name of the file, this string may only be intended to be 'machine-readable'.
  - FileSize - the (integer) size of the update file in bytes.
  - VendorSpecificInfo - information specific to the file, no format is specified for this information.
  - @ModuleType - the usage of this is currently unspecified.
- FootprintSize - the required resource for the update package, this includes:
  - @Volatile - the size (in bytes) of 'RAM' needed for the update package to be compatible in bytes.
  - @NonVolatile - the size (in bytes) of non-volatile storage needed for the update package to be compatible.
- ImagePackaging - Switches indicating that the image is packaged and signed, and whether a manifest is used, the states are defined as 0 = false, 1 = true. Neither signing nor use of manifest is defined in this version of the RMS-FUS specification (TS 102 824 [2]):
  - @SignedPackaging - "0"=false, "1"=true;
  - @Mainfest - "0"=false, "1"=true.
- UpdateDescriptor - this sub-structure is based on the DVB-SSU [3] methods and may be present to indicate how the update should be applied to the target device, it includes:
  - UpdateFlag - an indication as to whether the update must be carried out (manual or automatic).
  - UpdateMethod - An indication of when the update should be applied (immediate, user convenience or at next restart).

- UpdatePriority - priority, with values from 1 to 4, with lowest having greatest priority.

7.3.3 ValidityTimeRange

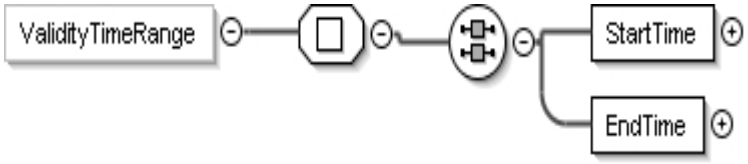


Figure 25: ValidityTimeRange Container

This contains 2 sub-elements defining the time window for the availability of the update package.

- StartTime - time/date in "dateTime" format specified in [10] when the update is first available.
- EndTime - time/date in "dateTime" format specified in [10] after which the update will no longer be available.

7.4 The main descriptive metadata

This clause gives a high level description of the metadata structure with some examples. The structure makes use of the element and group types defined above in appropriate combinations and each instance of the schema should allow a complete and unique description of a single firmware update file with information about the associated FUS assigned to deliver it and the RMS managing the process for managed CPEs. Information may be added, modified and removed at various stages through the lifecycle of the download file delivery.

7.4.1 Mode

The mode element is used to explicitly indicate whether a firmware update file is intended for managed or unmanaged CPEs.

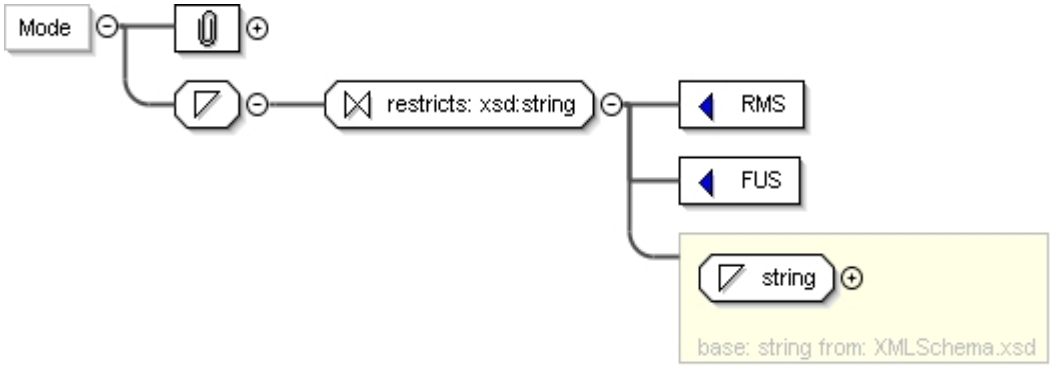


Figure 26: Mode information

7.4.2 Entity definitions

Four entity groups are defined, each carrying information appropriate to that part of the overall chain.

7.4.2.1 CE Manufacturer

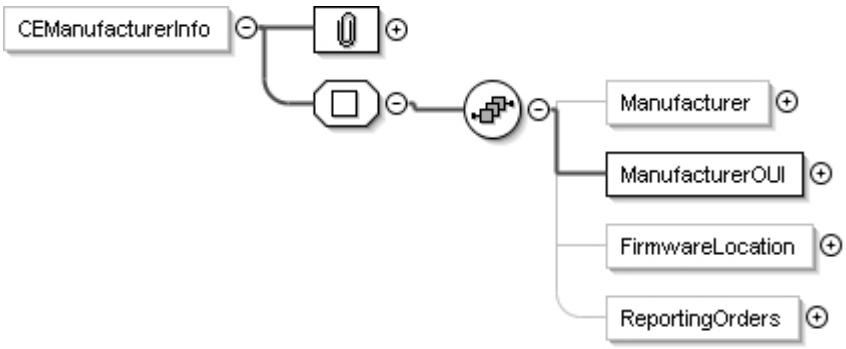


Figure 27: CE manufacturer information

This information is added by the CE manufacturer and is included to inform the FUS and RMS of the location from where a new firmware file can be downloaded. The Manufacturer is identified primarily by the OUI although the human readable name may be included.

The use of reporting orders is based on the DVB SSU specification TS 102 006 [3] and is used to carry an address to which unmanaged CPEs can report the results of a download, the location and specification of this communication is out of scope of the specification and it will be expected that the CPE will manage this exchange.

7.4.2.2 FUS

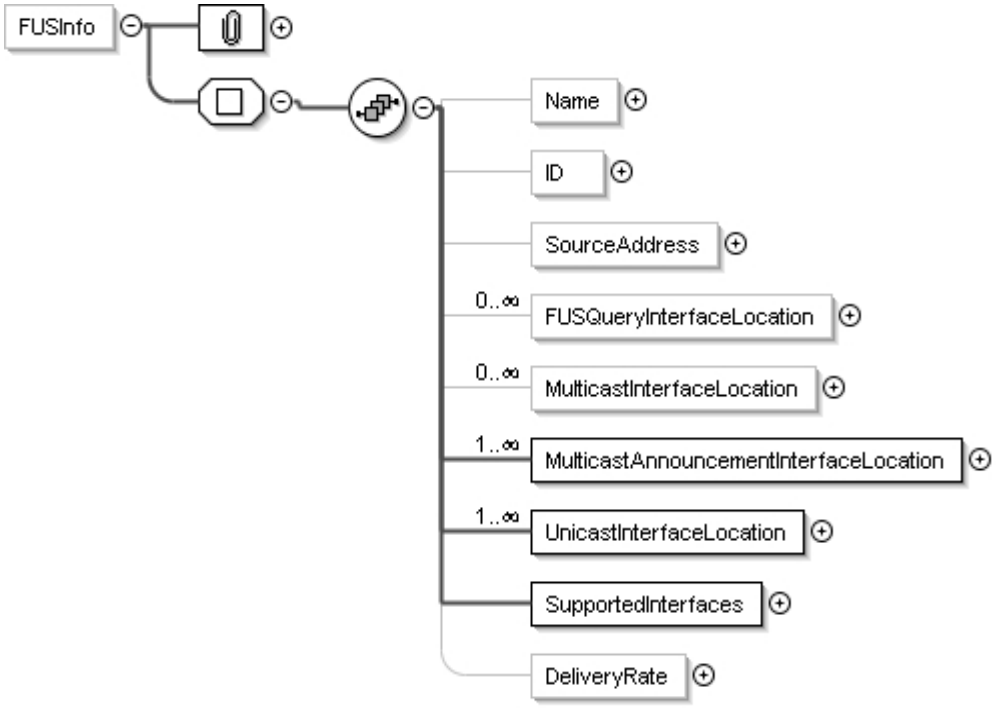


Figure 28: FUS information

This clause should be populated by the FUS and should describe the capabilities of the FUS in terms of compatibility with other entities and with delivery methods to the CPE.

The name and ID may be used to identify the FUS, the source address for the FUS may also be provided. The interfaces which are supported by the FUS are identified in list based on "SupportedInterfaces".

Since each XML instance is a unique description of information specific to a firmware update file the interface description elements (listed below) will indicate which interfaces are appropriate in each case.

- FUSQueryInterfaceLocation (QRC) - the address which should be used by the CPE if the query-response interface is to be the method used to discover a firmware update appropriate for the CPE.
- MulticastAnnouncementInterfaceLocation - this address range or list may be used to indicate the addresses which may be used to delivery announcements over multicast.
- UnicastInterfaceLocation - this address range or list may be used to indicate the addresses which may be used to delivery firmware updates over unicast.
- MulticastInterfaceLocation - this address range or list may be used to indicate the addresses which may be used to delivery firmware updates over multicast.

A field (DeliveryRate) is provided to allow the FUS to indicate the maximum file throughput rate for the FUS.

7.4.2.3 RMS

This information is only necessary when a firmware update image is being announced for a managed CPE.

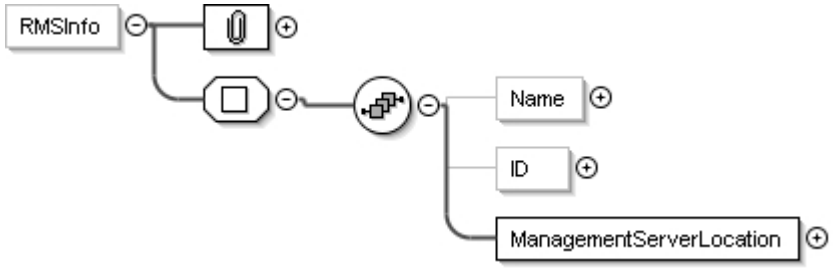


Figure 29: RMS information

Identification of the RMS may be carried in the human readable name and the ID fields. The primary RMS address shall be carried in the ManagementServerLocation field.

7.4.2.4 Target devices

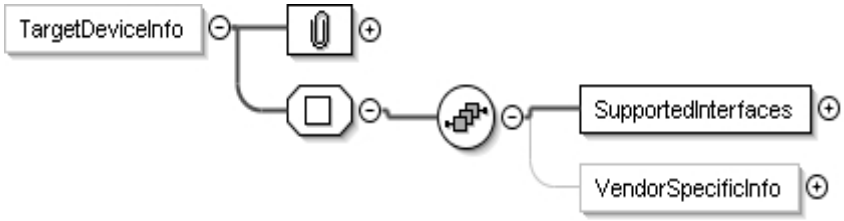


Figure 30: Target devices information

The SupportedInterfaces field carries a list of interface (from interfaces 5 to 9) which are supported on the FUS, thus allowing a CPE to carry out an interoperability check. FUS specific information can be provided in the VendorSpecificInfo, the format is undefined.

7.4.3 Firmware Upgrade information

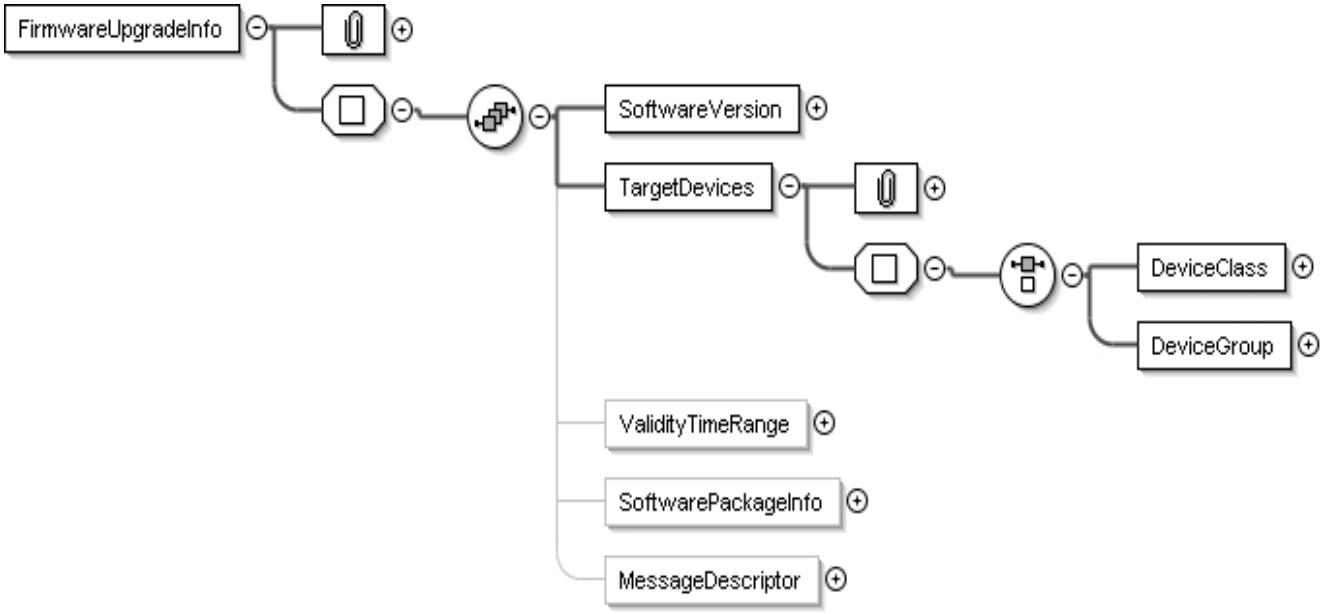


Figure 31: Target devices information

This clause of the metadata contains the description of the actual update file. The target devices are defined by device and current software, or by a potentially more detailed identification based on device class or device group. This latter group may include use of serial number information as well as current software and hardware versions.

The information provided will be based on the types defined in clauses 7.2 and 7.3, it includes:

- Software version - the version of the firmware update file described in clause 7.2.4.
- TargetDevices - this includes the capability to define the target CPE population by DeviceClass (described in clause 7.2.9) and/or DeviceGroup (a more precise method described in clause 7.3.1).
- ValidiltyTimeRange - indicating the date/times when the update package will be available using start and end times as the criteria, this is defined in clause 7.3.3.
- SoftwarePackageInfo - this metadata structure is defined in clause 7.3.2 and describes structure of and installation requirements for the update package.
- Messagedescriptor - this can be used to carry information about the update intended for the user, the semantics used for this are similar to those defined for DVB-SSU [3].

8 Security Considerations for CPE management operations

Security aspects of the RMS and FUS services are as specified in TS 102 824 [2], clause 5.4 and the relevant clauses in clause 6. Table 4 summarises the requirements defined in that document. The significant references for the TLS and SFTP methods used in tables 5 and 6 are:

- RFC 3268 [14];
- RFC 4346 [16];
- RFC 2246 [17];
- RFC 4217 [18];
- RFC 2818 [19];
- RFC 3852 [20].

Table 4: List of security capabilities for RMS-FUS

Capability	Broadband Forum	DVB
Interface 9 - CPE management interface		
SSL/TLS support		
SSL/TLS usage	RECOMMENDED	Refer to BBF TR-069 [7]
CPE support for SSL 3.0 and TLS 1.0	MUST	Refer to BBF TR-069 [7]
CPE support for SSL/TLS cipher suites RSA_WITH_3DES_EDE_CBC_SHA and RSA_WITH_RC4_128_SHA	MUST	Refer to BBF TR-069 [7]
CPE support for SSL/TLS cipher suites RSA_WITH_AES_128_CBC_SHA and RSA_WITH_AES_256_CBC_SHA	---	SHOULD
CPE to authenticate the ACS using the ACS-provided certificate in case of SSL/TLS	MUST	Refer to BBF TR-069 [7]
CPE contains one or more trusted root certificates	MUST	Refer to BBF TR-069 [7]
Provisioning of trusted root certificates	Out of scope	Refer to BBF TR-069 [7]
CPE authentication using client-side certificates with unique or generic CPE client certificates	OPTIONAL for both the CPE and ACS	Refer to BBF TR-069 [7]
If generic CPE client certificates are used the ACS to additionally authenticate the CPE using HTTP basic or digest authentication	SHOULD	Refer to BBF TR-069 [7]
HTTP authentication		
CPE support for both HTTP basic and digest authentication	MUST	Refer to BBF TR-069 [7]
ACS to request HTTP digest authentication if SSL/TLS is not used	MUST	Refer to BBF TR-069 [7]
Globally unique username/userid among all CPE manufacturers	SHOULD	Refer to BBF TR-069 [7]
Globally unique password among all CPE manufacturers	SHOULD	Refer to BBF TR-069 [7]
Provisioning of the password	Out of scope	Out of scope, MAY be done by means of Factory default configuration. Local configuration (e.g. via a GUI or a Smart Card). Configuration using the RMS interface
Interface 1 - Firmware Update file from CE manufacturer to FUS manager		
Encoding or encryption of the firmware update file by the vendor		MAY

Capability	Broadband Forum	DVB
Interface 5 - Multicast delivery of firmware update file to network		
Authentication of the server		RECOMMENDED (i.e. authentication of the firmware update file)
Encoding or encryption of the firmware update file by the vendor		SHOULD
Packaging of the image and the use of an additional signature		MAY
Interface 6 - Unicast delivery of firmware update file to network		
Authentication of the server and the client		RECOMMENDED
HTTP and HTTPS support		MUST (CPE) OPTIONAL (FUS)
SFTP, FTP and TFTP support		OPTIONAL
SSL/TLS usage details and authentication details for the used protocols		Refer to interface 9
Encoding or encryption of the firmware update file by the vendor		SHOULD
Packaging of the image and the use of an additional signature		MAY
Interface 7 - Firmware Update announcement service		
Authentication of SAP announcements		RECOMMENDED Detail of method is specified in TS 102 824 [2] clause 6.7.2.1.2
Encryption of SAP payload for administratively scoped sessions		Not applicable.
Authentication of DVBSTP announcements		Not applicable NOTE: Since the transport is multicast, the authentication of the message exchange is problematic but the defence for the interface is the authentication of the payload package (or file).
Interface 8 - Query/response interface from FUS to home environment (QRC)		
SSL/TLS		RECOMMENDED
SSL/TLS usage details and authentication details for the used protocols		Refer to interface 9
		As described in clause 6.8.3 of TS 102 824 [2], the CPE should in addition authenticate the package (or file) itself.
Other security features		
Network time security		
Secure network time using NTP v3		SHOULD

Table 5: Required compliance with ciphersuites for QRC and RMS

Ciphersuite	Query Response Service (Interface 8)	Remote Management Service (Interface 9)
RSA_WITH_RC4_128_SHA	C(M)	C(M)
RSA_WITH_3DES_EDE_CBC_SHA	C(M)	C(M)
RSA_WITH_AES_128_CBC_SHA	C(S)	C(S)
RSA_WITH_AES_256_CBC_SHA	C(S)	C(S)

The notation used is:

C(M) = If the interface supports TLS:TCP:IP, support this ciphersuite is mandatory.

C(S) = If the interface supports TLS:TCP:IP, the interface should support this ciphersuite.

9 Use of "dvb-mcast" URI

A DVB URI schema is specified in TS 102 851 [25] to describe delivery of services using multicast methods. It was specifically designed to cover cases where multiple alternative delivery protocols may be allowed and where additional information is needed to complete the delivery. The detailed schema is extended in TS 102 034 [1], clause 10 and in TS 102 824 [2] for the SDP/SAP/UDP and DSMCC cases.

Examples of how this might be used in the scope of RMS-FUS are given in clauses 9.1 and 9.2.

9.1 Example describing location of multicast announcement message using SDP/SAP/UDP

In this case the detail of the schema is extended in TS 102 034 [1], clause 10 for the delivery of the announcement messages over SDP/SAP/UDP.

The URI "dvb-mcast://dvb-fus@240.0.0.51:32000?payload=sap" points to a SAP/SDP announcement. The announcement is delivered from the host named dvb-fus using the IPv4 multicast address 240.0.0.51 to port 32000. The announcement is targeted for manufacturers which OUI are 00D09D, 00D09E and 00D09F and announces a single channel FLUTE session that would eventually deliver the firmware update.

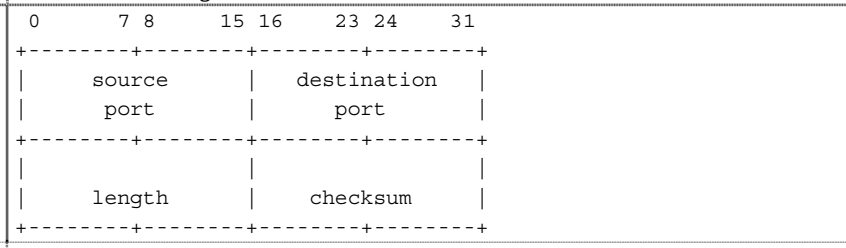
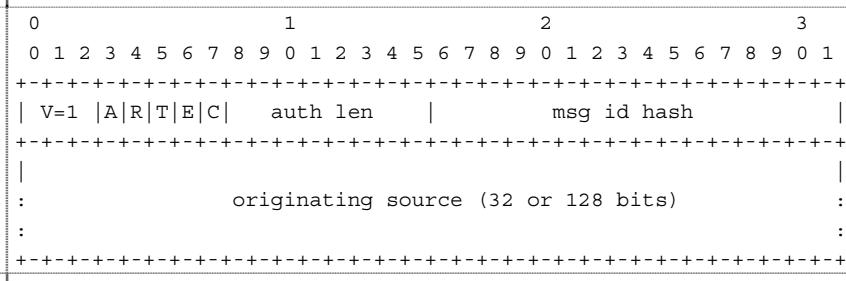
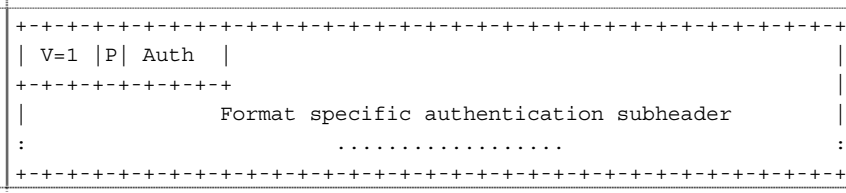
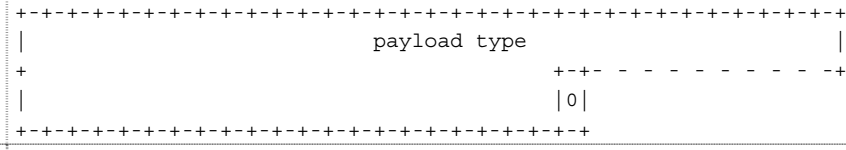
Protocol / Field	Format and encoding	Remark
UDP		The destination port in this example would be 32000. The source port is determined by the announcement server. The length field supplies length of the UDP data comprising SAP and SDP data as shown below.
SAP		SAP is specified in [22]. The SAP profile for DVB announcements is given in [2], clause 6.7.2.1.
SAP (authentication data)		The authentication data are optional and a profile is given in [2], clause 6.7.2.1.
SAP (payload type)		The payload type is mandatory and always set to "application/sdp".
SDP	v=0 o=dvb-fus 2890844526 2890842807 IN IP4 10.47.16.5 s=dvb-update t=2873397496 2873404696 a= x-dvb-rms-ce-manufacturer:00D09D 00D09E 00D09F	SDP is specified in [23]. This example SDP message is sent by a FUS named "dvb-fus" having IP address 10.47.16.5. The announcement is intended for manufacturers which OUI are 00D09D, 00D09E and 00D09F.
SDP (media section)	m=application 49153 FLUTE/UDP * c=IN IP4 240.0.0.3 a= flute-tsi:142 a= source-filter: incl IN IP4 * 192.168.1.1	In this example a single channel FLUTE session is announced with destination port 49153 and multicast IPv4 address 240.0.0.3. The FLUTE data stream will be sent from the address 192.168.1.1 and is identified by the TSI=142.

Figure 32: Example multicast announcement over SDP/SAP/UDP

9.2 Example describing location of multicast update file using DSM-CC/UDP

The DVB URI schema specified in TS 102 851 [25] is extended in TS 102 824 [2], clause C.4 to describe delivery of services using DSMCC over multicast IP methods using the "dvb-mcast" URI format. It was specifically designed to cover cases where multiple alternative delivery protocols may be allowed and where additional information is needed to complete the delivery.

Because the DSMCC payload is carried as MPEG2-TS packets the payload type used is "mp2t".

The simplest form of the URI as below points to a DSMCC download announcement not using SSM, therefore not requiring the source address, and delivered from the host multicast address 240.0.0.51 to port 32000. No other specific information is provided for the service in this case.

dvb-mcast://240.0.0.51:32000?payload=mp2t

Where:

- Host multicast address = 240.0.0.51.
- Port = 32 000.
- Payload type = "mp2t".

This can be extended to include more precise information about the DVB service where the download can be located, allowing the location of the download within one of multiple carousels carried in a single DVB service to be known without examining every carousel, and for the download location to be advertised when multiple DVB services carry carousel components. The schema structure is described in TS 102 851 [25], profiled in TS 102 824 [2]. A more complex example which also provides the service id and carousel id is shown below.

dvb-mcast://240.0.0.51:32000?payload=mp2t&0202$045F1A23

Where:

- Host multicast address = 240.0.0.51.
- Port = 32 000.
- Payload type = "mp2t".
- Service id = 0x0202.
- Carousel id = 0x045F1A23.

10 Possible CPE behaviour examples for RMS and FUS

This clause contains some examples of how a DVB CPE can carry out Firmware Update by making use of the resources specified in the DVB IPTV Handbook TS 102 034 [1] and the RM-FUS specification document (TS 102 824 [2]). It should be noted that the scope of the firmware update description features available using an announcement over SDP/SAP/UDP and use of the XML description delivered over DVBSTP/UDP can differ. Some extended features are only available when the XML/DVBSTP/UDP is used. Those extended features are optional parts of the metadata structure which are not carried in the SDP attributes specified in TS 102 824 [2]. A more detailed description is provided in clause 11.1.1.2 and can be used in either managed or unmanaged CPEs and for boot or normal operation if the XML/DVBSTP/UDP location methods are used.

Firmware Update is primarily made up of two steps:

- Firmware download.
- Firmware application.

This may possibly be followed by a CPE reboot. Generally firmware download is not disruptive, but any run time firmware update and consequent reboot are likely to disturb the user's viewing experience since they break the CPE operation flow.

The moment when the CPE starts applying the firmware update is not under control of the FUS and only partially under control of the RMS.

As outlined in clause 5, RMS and FUS can exist independently of each other and each of them can operate in a standalone mode.

As far as the RMS is concerned, the TR-069 [7] Remote Management framework specified by BBF can implement a standalone Firmware Update functionality of its own. The CWMP specification of Firmware Update includes downloading and applying the Firmware, where Firmware is considered to have been applied when installed and in use as intended.

RMS and FUS can also be active at the same time and co-operate providing additional functionality to the user for both servers over the standalone modes. For CWMP, for instance, specific RPCs such as the AUTONOMOUSTRANSFERCOMPLETE are only for RMS-FUS operation, this functionality is additional to that used in the standalone RMS Firmware Update using the TR-069 mechanism.

The central role of the RMS in the set of possible operation modes also suggests that CPEs can be more simply grouped as follows:

- Managed CPEs, supporting the following usage modes:
  - RMS-only, this also includes any modes defined within relevant remote management specifications, e.g. TR-069, Cablelabs PACM;
  - RMS-FUS, where the features defined in the remote management specifications are extended by those described in TS 102 824 [2].
- Unmanaged CPEs, supporting the following usage mode:
  - FUS-only, where CPEs obtain firmware updates using the metadata structure supported in TS 102 824 [2] as a method of locating appropriate updates.
- What is more, in what follows for each CPE family two operational conditions are considered:
  - Boot Time;
  - Normal operation.

10.1 At Boot Time

To properly perform Firmware Update DVB CPEs need the entry points for the FUS service and, if available, the RMS service.

The FUS entry points, i.e. the URLs of the multicast announcement and the QRC servers are usually provided at boot time by means of the FUSS (FUS Stub) file. DVB-IPTV CPEs are always expected to download the FUSS file, so they need to discover the URL where the FUSS file resides The procedures to retrieve the FUSS file are specified in clause 9 of the IPTV Handbook (TS 102 034 [1]) and described in clause 5.3 of the core IPTV Guidelines - Part 1 of the present document.

The FUSS file contains identification data for the device and a URL / IP address for the CPE to connect to the FUS system. The example structure used in the FUSS, including the short form encoding, is contained in table 23 of the Handbook (TS 102 034 [1]), clause 9.2.

The entry point for the RMS service is the address of the RMS server. The RMS system is specified outside DVB, so the way to provide the DVB CPE with this address at boot is found first of all in the relevant RMS specification, for example, BBF TR-069 (CWMP) specifies a procedure at boot time based on the exchange of DHCP options (TR-069 [7], clause 3.1). It should be noted that the DCHP based procedure for acquiring this RMS address is similar to that specified to get the URL of the FUSS file.

As a further option the entry points for FUS and RMS services could be hard coded in the CPE firmware.

After getting the RMS and FUS addresses the CPE checks whether a Firmware Update is required. According to whether the CPE is managed or unmanaged this may take place in different ways:

a) For Unmanaged CPEs:

   1) Listening for an announcement to a multicast group from a FUS announcement server, getting the Firmware Update unicast or multicast address and download it. The mechanisms to deliver announcements and files via multicast or unicast connections are specified in the Handbook (TS 102 034 [1]) clause 5.6 and illustrated in clauses 11 and 12. This mechanism works at boot time as well as during normal operation.

   2) Querying the unicast FUS QRC server, getting information about when and at which multicast group/ unicast server a download is available and downloading it from the (unicast or multicast) URL provided. This mechanism works at boot time as well as during normal operation.

b) For managed CPEs:

1) If a FUS system is present together with the RMS, the previous options hold.

2) RMS-specific download functionalities are also available, for RMS-only as well as RMS+FUS systems. For CWMP the standalone functionality is implemented with the DOWNLOAD RPC that causes the CPE to connect to the (unicast or multicast) URL specified by the RMS and retrieve the file. As before, the URL specified by the RMS may point directly to the Firmware file(s) or indirectly to a URL where the CPE is redirected to retrieve the Firmware file(s).

Finally, after downloading and applying the Firmware Update, the CPE may need to reboot.

As a standard management operation, then, the CPE notifies the RMS of the new Firmware version applied. This may cause the RMS server to reconfigure and in some cases may also require (generally limited) changes to the CPE data model.

10.2 During Normal Operation

After the boot process is complete the CPE runs in the normal operational mode, discovering services through SD&S multicast channel, if available, and providing content and associated services to the user.

The SD&S flow contains a specific record (PayloadID = 0x08) designed to support RMS-FUS including the specification of the entry points for FUS and RMS. The SD&S record may be used to obtain the RMS and FUS addresses in the absence of a FUSS file at boot time. Also, the presence of this RMS-FUS record within the SD&S DVB-IPTV framework provides operators/ service providers with the technical possibility to change RMS and FUS servers at run time. However, for CPEs managed using the BBF CWMP framework, the CPE behaviour when the RMS server changes is specified in TR-069 [7], table 7 for the protocol details and TR-106 [8] for the data model support.

Any CPE, whether managed or unmanaged, may at any time (based on the CPE policy) check for new Firmware Updates by accessing the FUS and / or RMS servers that are configured at the time. The time that this may take place (periodically, at boot time or upon specific events) is dictated by the CPE policy.

For unmanaged CPEs, different mechanisms are available to check for Firmware Updates: the CPEs can either examine the multicast announcement channel or query the unicast QRC server. The FUS server indicated can be multicast or unicast. Different CPE classes can make use of different mechanisms (multicast/ unicast) to check for Firmware Updates.

Mitigation strategies can be implemented in the servers to assist if any CPEs have problems downloading firmware updates, these strategies may differ between managed and unmanaged CPEs and some options are described in clause 11.1.1.2.

10.2.1 RMS-only

For managed CPEs with no FUS the Firmware Update is provided by RMS specific mechanisms. In the case of BBF TR-069 framework the RMS server is able to request the execution of a Firmware Update to the CPEs that are in need of it. The RMS request specifies which download server the CPE should use. The CPE is required to notify the RMS of the completion status (successful/unsuccessful) of the Firmware Update (Downloaded and Applied).

Managed CPEs that carry out the Firmware Update upon explicit RMS server request are usually forced to comply with the time limits set by the RMS server for this operation. The RMS usually tends to set time limits and force all procedures to complete in a known time interval in order to keep network management under control. From the RMS point of view this is of the utmost importance, to such an extent that achieving this goal may lead, in extreme cases, to disrupting the user experience. To correctly manage a CPE, what is more, the RMS generally needs to know which Firmware version the CPE is running. Where TR-069 is the standard on which the management is based the RMS is notified of this by the CPE after the CPE applied the firmware, including reboot if necessary.

It should be noted that in the case of managed CPEs, they are quite unlikely to request Firmware Update autonomously, since it is reasonably expected that this maintenance activity would be carried out by RMS systems. However, user-requested Firmware Update might still have some meaning, for instance as a basic case of self-managed troubleshooting, and is supported where TR-069 is the standard on which the management is based.

The run time use cases described match those described at boot time, although more options are available:

1) The Firmware Update could be requested by the user himself.

2) The Firmware Update could be requested by a LAN-side manager (e.g. UPnP).

It has to be noted that in the case of managed CPEs the user is quite unlikely to requested Firmware Update by himself, since they reasonably expect this maintenance activity to be carried out by RMS systems. User-requested Firmware Update might still have some meaning, though, for instance as a basic case of self-managed troubleshooting.

10.2.2 RMS-FUS

When both CWMP and FUS are implemented all the use cases previously mentioned still apply, but there is an additional method in which the RMS carries out the Firmware update by configuring the FUS system through the RMS-FUS interface, shown as Interface 4 in figure 1, rather than configuring the CPEs. The FUS system is configured by the RMS to broadcast new announcements and new Firmware updates for one or more CPE classes. Interface 4 is out of scope of the FUS specification and these guidelines since it is a B2B interface. In this case the CPEs involved in the Firmware Update may optionally notify the RMS server, according to their policy, of the completion status of the Firmware Update. The Firmware Version parameter is specified by TR-106 [8] to be included in every CWMP message (INFORM) sent by the CPE to the RMS to start a new management session, so the RMS server is notified about the new firmware version at the beginning of next management session at the latest.

CPEs that download the firmware autonomously may be able to choose the most suitable moment to apply the Firmware so as to minimize disruption of the user's experience unless the metadata provided by the FUS in the multicast announcements indicates that an immediate download and installation is required, this is included in the fields of the "UpdateDescriptor" which is part of the "SoftwarepackageInfo" grouping. More description is given in clause 11.1.1.2. This is only supported for metadata delivered as XML/DVBSTP/UDP.

10.2.3 FUS-only

For DVB FUS based systems the CPE must acquire the information about the firmware update from the FUS. This can be done either by listening on the multicast announcement service available over either SDP/SAP/UDP or XML/DVBSTP/UDP, or by using the unicast QRC interface to initiate the communication the FUS with CPE specific queries. The FUS will not initiate unicast communications with any CPE.

If the XML/DVBSTP/UDP multicast service is used the extended features described in clause 11.1.1.2 can be used if the fields are populated.

The DVB FUS specification does not say anything about applying the firmware, which is left totally under control of the CPE policy. The CPE may then have a certain degree of freedom in the selection of the best moment to reboot in order to minimize the user's inconvenience if the metadata contains the appropriate field values, this is described in clause 11.1.1.2.

11 Location of firmware update files

This clause provides an illustration of the protocols used:

- The multicast announcement.
- The unicast QRC query.
- The management (based on the TR-069 framework [7]).

All the navigation methods based on the FUS may be used by either managed or unmanaged systems but it is assumed that the unicast QRC mechanism will not be used since it is an unmanaged equivalent to the TR-069 management service in the sense of firmware updates. Navigation based on the management interface (interface 9) cannot be used in the absence of any RMS (i.e. unmanaged CPEs) and it is expected that only a subset of the FUS methods available will be used by the managed systems.

An FUS may be providing multiple download streams on multiple IP addresses, in both multicast or unicast, and each multicast service carousel may contain multiple download image files. Also, using the full scope of the metadata available for a CPE update where the XML/DVBSTP/UDP announcements are monitored allows some extended features to be used as described in clause 11.1.1.2.

11.1 Unmanaged environments - FUS-only

In unmanaged environments only multicast announcement and unicast QRC access are available.

11.1.1 Use of multicast announcement service

The multicast announcement information can be carried in two formats:

1) SDP/SAP coding over UDP, for which a security profile was specified in TS 102 824 [2], clause 6.

2) XML over DVBSTP/UDP.

They will be illustrated in the following clauses.

11.1.1.1 Use of SDP/SAP/UDP Protocol

SDP is carried on top of SAP/UDP. SAP based on RFC 2974 [22] mainly specifies the general characteristics of the SDP payload, such as payload length and whether it is encrypted. SDP describes in detail an SDP announcement session, i.e. a set of announcements delivered at the same time. These announcements correspond to real files to be downloaded. Each SDP session announcement needs to identify:

1) The multicast group which the CPE should join to download the Firmware Upgrade.

2) Which protocol /(FLUTE/DSM-CC) it must use.

3) For which CPEs this Firmware download is intended.

All this information may be conveyed by means of a combination of SDP fields (mainly m=, c=, and a=) as shown in Annex D of the RMS-FUS specification TS 102 824 [2]. The SDP attribute structuring is based on the XML which can be delivered using the DVBSTP/UDP protocol as in clause 11.1.1.2.

11.1.1.2 Use of XML/DVBSTP/UDP Protocol

The XML is carried over DVBSTP/UDP using the PayloadID 0xB2, the SegmentID may be different for each description document. This method can also carry the full XML description document for each update file, and may include:

- The ability to identify all the component files for updates which require multiple parts in a vendor specific way in the "module" attribute (string format) of the "PackageFile" section of the "SofwarePackageInfo", as described in, The XML document structure is provided in annex 2 of the RMS-FUS specification [2] and is described in clause 9 of the present document.

- The ability within the XML structure to allow the definition of multiple interfaces for the FUS for both multicast and unicast interfaces (or a mix of both), with a "preference" attribute being available to indicate the priority which should be given to it by the CPE. This can be used to implement a recovery strategy for CPEs having difficulties downloading an update by any single method. This option to carry multiple interface URLs may only be supported in the carriage of XML over the DVBSTP/UDP multicast protocol. No specific unicast recovery mechanism is defined in the RMS-FUS specification.

- The fields of the "UpdateDescriptor" which is part of the "SoftwarepackageInfo" grouping support some behaviour inherited from the DVB SSU specification, including:

  - "UpdateFlag" indicating whether the CPE should have an option about the timing of the update.

  - "UpdateMethod" indicating when the CPE should carry out the update.

  - "UpdatePriority" indicating the importance given to the update by the manufacturer.

- Fields describing the time period for which the firmware update will be available may be provided in the "FirmwareUpgrade.ValidityTmeRange.StartTime" and "FirmwareUpgrade.ValidityTmeRange.EndTime".

11.1.2 Use of Unicast Query-Response Channel

The Unicast Query-Response Channel is a simple unicast interface through which the CPE tries to connect to the QRC server to retrieve information about available Firmware Updates. The protocol stack is SOAP as defined in [9] over HTTP or HTTPS. Two Remote Procedure Calls (RPCs) are defined over SOAP: FirmwareUpdateCheck and FirmwareUpdateCheckResponse.

The QRC server may request the CPE to authenticate through the HTTPS Challenge-Response mechanism. This takes place (at the HTTP level) when the QRC server receives a FirmwareUpdateCheck RPC. The FirmwareUpdateCheck RPC contains arguments that allow the RMS to identify the requesting CPE.

After completing the authentication procedure the QRC server identifies the CPE and determines whether there are any Firmware Updates for the requesting CPE. The RMS responds with a list of URLs containing the relevant file(s). The list is empty if no Firmware Update is available.

11.2 Managed environments - RMS-FUS

It is assumed that the CPE and FUS will be configured as necessary by the RMS in all managed environments, although the mechanism for that operation is only described in the present document for cases where TR-069 [7] is used.

11.2.1 Use of management channel (TR-069 methods)

As explained in clause 9, both options with FUS present and missing must be taken into account. Regardless of the FUS being present or not, the RMS carries out all the usual management tasks on each CPE, including but not limiting to Firmware Update, and is informed by each individual CPE about the completion status of any management activity, including the Firmware Update.

A managed CPE uses the RMS entry point information to discover the RMS server it has to connect to for initial configuration. Firmware Update may or may not be part of this initial configuration. A non exhaustive list of example options is as below:

1) The RMS determines that the CPE needs Firmware Update and request the CPE to download and apply Firmware as a part of the boot procedure. In this case the download server does not need to be a FUS server. The download server may be unicast as well as multicast. When the Firmware Update is complete the CPE notifies the RMS server about the completion status (successful/unsuccessful) of this activity with a TRANSACTIONCOMPLETE RPC.

2) The RMS might determine that the CPE needs Firmware Update and, in a system that includes FUS, request the FUS to advertise the Firmware version required by this CPE. The interface between RMS and FUS is out of scope of the present document. In this case the CPE terminates the boot with no firmware update- As soon as the CPE starts normal operation it joins the announcement multicast group, discovers the new Firmware version available and performs the Firmware Update at that time. When the Firmware Update is complete the CPE notifies the RMS server about the completion status (successful/unsuccessful) of this activity with an AUTONOMOUSTRANSFERCOMPLETE message.

12 Delivery of Firmware Update Files

12.1 Multicast Download

The multicast protocols allowed by the FUS-RMS specification are FLUTE [15] and DSM-CC [4]. The usage is profiled in clause 6.5 of TS 102 824 [2].

12.1.1 Use of FLUTE Protocol

FLUTE session can be used for downloading the Firmware for a CPE. The parameters of the FLUTE Sessions (e.g. multicast channel information, FLUTE TSI) are provided by the relevant FUS announcements. Mandatory support of the "Compact No Code FEC scheme" as defined in RFC 3452 [13] and of a single multicast channel per FLUTE session is required. Other FEC schemes and multiple multicast channels per FLUTE sessions can be optionally supported, however the currently defined SDP and XML attributes and structures for FUS announcements do not support the announcement of the necessary information for FEC and multiple multicast channels. For example the SDP announcement of multiple multicast channels per FLUTE session would require a media description (m-line) per multicast channel. Currently however media descriptions present an announcement message for a target population of CPEs.

12.1.2 Use of DSM-CC Protocol

Further details on DSM-CC can be found in the DVB RMS-FUS Specification [2], based on the DSM-CC specification [4]. The use of the mcast-URI (see DVB RMS-FUS Specification [2], clause C.4) allows identifying the specific DSM-CC carousel within the MPEG-2 transport stream.

12.2 Unicast Download

Unicast protocols allowed by the FUS-RMS specification TS 102 824 [2] are HTTP, HTTPS, FTP, TFTP, used as profiled in the IPTV Handbook TS 102 034 [1], where the specifications to these protocols are referenced.

13 Remote Management functions for CDS

DVB CDS supports push and pull download service modes. In the push download service mode the download of content items to the local storage of a HNED is initiated by the service provider, without explicit request by the user. In the pull download service mode the download is initiated at the explicit request from the user.

The CDS service provides a limited set of content and storage management functionality. Those functions are described in clause 10.7 of TS 102 034 [1].

The management functions provided via RMS which are used to manage the CDS are described in annex F of TS 102 824 [2]. The RMS management functions allow the configuration of the CDS storage space when the CDS service has been newly introduced, or when a STB connects to the provider's network for the first time. Furthermore targeted deletion of content items is possible to free storage space if e.g. for some reason content items have not been deleted via the regular CDS deletion function.

The DVB extensions for the STB data model are shown using red characters in figure 33, which is based on figure 2 of TR-135 [6] - STBService Object Structure and figure 1 of TR-140 [5] - StorageService Object Structure.

According to TR-135 [6] the PVR.Storage object is a multiple instance object. The single instances refer to either TR-140 [5] StorageService instance, or an object contained within such an instance, i.e. a PhysicalMedium, a LogicalVolume, or a Folder. As further explained in clause F.1 of TS 102 824 [2] it is recommended to implement the storages for PVR, CDS Push and Pull services as folder objects since storages such as complete partitions are not resizable via remote operations. The arrows in figure 33 illustrate to where the different service storages may refer to. However this should be considered as an example only and an actual implementation may differ.

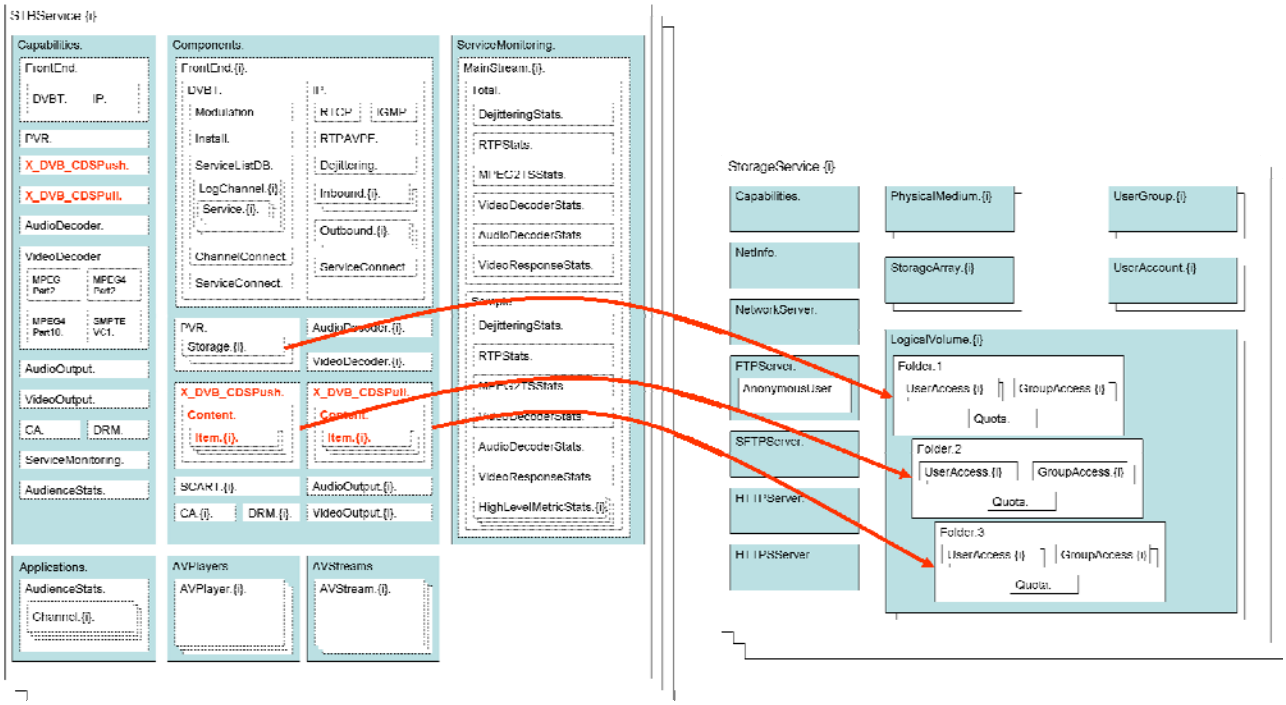


Figure 33: Object model for CDS

For the CDS Push service storage the following management methods have been defined:

- Query if the HNED provides a CDS Push service storage space

  `.STBService.{i}.Capabilities.X_DVB_CDSPush.CDSPushCapable`: This flag is set to 'TRUE' by the HNED if the CDS Push service with the associated storage space is supported with the current software.

- Query and modify the overall CDS Push Service storage space

  `.STBService.{i}.Components.X_DVB_CDSPush.Reference`: This parameter references an object contained within a TR-140 StorageService instance, e.g. a PhysicalMedium, LogicalVolume or Folder instance.

  Modification of the storage space via CWMP is only possible if the CDS Push service storage is implemented as a folder object in the HNED since storages such as complete partitions are not resizable via remote operations. Therefore it is recommended to follow the guidelines listed in clause F.1 of TS 102 824 [2].

- Query the used CDS Push Service storage space

  The `.STBService.{i}.Components.X_DVB_CDSPush.Reference` parameter is used to retrieve the full hierachical name of the actual TR-140 StorageService instance or an object within this instance. Eventually the TR-140 object the capacity/used space parameter of this StorageService object provides the requested information.

- Query the list of content items stored on the CDS Push Service storage space (this provides the content identifier and version number)

  A partial path name as e.g.

  `.STBService.1.Components.X_DVB_CDSPush.Content` is used in the GetParameterValues RPC to retrieve a content item list. Each content item object provides the following two parameters:

  `.STBService.{i}.Components.X_DVB_CDSPush.Content.Item.{i}.ContentReferenceId`: This is the ContentReferenceId as defined in TS 102 822-2 [24].

  `.STBService.{i}.Components.X_DVB_CDSPush.Content.Item.{i}.VersionNumber`: This is the content version number as defined in TS 102 034 [1].

- Delete individual content items on the CDS Push Service storage space

  The DeleteObject RPC for the appropriate content item object instance e.g. `.STBService.{i}.Components.X_DVB_CDSPush.Content.Item.5` shall delete all files associated with this content item, i.e. not only those that have been downloaded by the HNED in conjunction with the CDS service. Those files for example include items that have been generated on-the-fly by the video player during playback, or files for the storage of bookmarks.

The CDS Pull Service storage is usually managed by the user. However by configuration from the user the service provider can be allowed to manage the storage via RMS.

The following management methods shall be supported per individual HNED:

- Query if the HNED provides a CDS Pull service storage space

  `.STBService.{i}.Capabilities.X_DVB_CDSPush.CDSPullCapable`: This flag is set to 'TRUE' by the HNED if the CDS Push service with the associated storage space is supported with the current software.

- Query if the CDS Pull Service storage management via RMS is enabled

  In contrast to the CDS Push Service for CDS Pull the user has to explicitly agree that the operator is allowed to manage the service storage either as part of a contract or for help desk issues, e.g. when the user complains about missing storage space for further downloads. It is assumed that enabling of this capability is controlled via a local GUI displayed on the TV screen.

The following management methods apply only if CDS Pull Service storage management via RMS is enabled:

- Query and modify the overall CDS Pull Service storage space

  .STBServices.{i}.Components.X_DVB_CDSPull. Reference:

  Modification of the storage space via CWMP is only possible if the CDS Push service storage is implemented as a folder object in the HNED since storages such as complete partitions are not resizable via remote operations. Therefore it is recommended to follow the guidelines listed in clause F.1 of TS 102 824 [2].

- Query the used CDS Pull Service storage space

  The `.STBService.{i}.Components.X_DVB_CDSPush.Reference` parameter is used to retrieve the full hierachical name of the actual TR-140 StorageService instance or an object within this instance. Eventually the TR-140 object the capacity/used space parameter of this StorageService object provides the requested information.

- Query the list of content items stored on the CDS Pull Service storage space (this provides the content identifier and version number)

  A partial path name as e.g.

  `.STBService.1.Components.X_DVB_CDSPull.Content` is used in the GetParameterValues RPC to retrieve a content item list. Each content item object provides the following two parameters:

  `.STBService.{i}.Components.X_DVB_CDSPull.Content.Item.{i}.ContentReferenceId`: This is the ContentReferenceId as defined in TS 102 822-2 [24].

  `.STBService.{i}.Components.X_DVB_CDSPull.Content.Item.{i}.VersionNumber`: This is the content version number as defined in TS 102 034 [1].

- Delete individual content items on the CDS Pull Service storage space (this deletes all files that belong to the content item)

  The DeleteObject RPC for the appropriate content item object instance e.g. `.STBService.{i}.Components.X_DVB_CDSPull.Content.Item.5` shall delete all files associated with this content item, i.e. not only those that have been downloaded by the HNED in conjunction with the CDS service. Those files for example include items that have been generated on-the-fly by the video player during playback, or files for the storage of bookmarks.

History

Document history		
V1.1.1	November 2006	Publication as TR 102 542
V1.2.1	April 2008	Publication as TS 102 542
V1.3.1	June 2010	Publication
V1.3.2	May 2011	Publication