

ETSI TS 102 825-3 V1.2.1 (2011-03)

Technical Specification

Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 3: CPCM Usage State Information



ReferenceRTS/JTC-DVB-252-3

Keywordsbroadcast, DVB

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/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2011.

© European Broadcasting Union 2011.

All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM, **TIPHON**TM, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

LTETM is a Trade Mark of ETSI currently being registered for the benefit of its Members and of the 3GPP Organizational Partners.

GSM[®] and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	5
Foreword.....	5
Introduction	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	6
3 Definitions and abbreviations.....	7
3.1 Definitions	7
3.2 Abbreviations	7
4 Usage State Information General Requirements	7
4.1 Definition and application	7
4.2 CPCM Content Licence.....	7
4.3 Secure Binding to Content	8
4.4 Content Entering DVB CPCM System	8
4.5 Content within DVB CPCM System	8
4.6 Propagation Controls.....	9
4.7 Content Exported/Output from the CPCM System to a Trusted or Controlled CPS	11
4.8 Content Exported from the CPCM System to an Untrusted Space	11
4.9 Extensions	11
5 Overview of USI Fields.....	12
6 Detailed Description of USI Fields	13
6.1 Copy and Movement Control	13
6.1.1 Copy Control Information (CCI)	13
6.1.2 Copy Control Not Asserted (CCNA).....	13
6.1.3 Copy Once (C1)	13
6.1.4 Copy No More (CNM)	13
6.1.5 Copy Never (CN) Zero Retention Not Asserted	13
6.1.6 Copy Never (CN) Zero Retention Asserted	14
6.2 Consumption Control	14
6.2.1 Viewable (V)	14
6.2.2 View Window	14
6.2.2.1 View Window Activated (VWA).....	14
6.2.2.2 View Window Start.....	14
6.2.2.3 View Window End.....	15
6.2.3 View Period	15
6.2.3.1 View Period Activated (VPA).....	15
6.2.3.2 View Period From First Playback	15
6.2.4 Simultaneous View Count	15
6.2.4.1 Simultaneous View Count Activated (SVCA)	15
6.2.4.2 Simultaneous View Count.....	15
6.3 Propagation Control	16
6.3.1 Movement and Copying Propagation Information	16
6.3.1.1 Movement and Copying Within Localized AD Enabled (MLAD)	16
6.3.1.2 Movement and Copying Within GAD Enabled (MGAD).....	16
6.3.1.3 Movement and Copying Within AD Enabled (MAD)	16
6.3.1.4 Movement and Copying Within CPCM Enabled (MCPCM).....	16
6.3.2 Viewing Propagation Information	16
6.3.2.1 Viewing Within Localized AD Enabled (VLAD).....	17
6.3.2.2 Viewing Within GAD Enabled (VGAD)	17
6.3.2.3 Viewing Within AD Enabled (VAD).....	17
6.3.2.4 Viewing Within CPCM Enabled (VCPCM)	17

6.3.3	Transition from "LAD or GAD Usage" to "AD Usage"	17
6.3.3.1	Remote Access Rule	17
6.3.3.2	Remote Access Date flag (moving window).....	18
6.3.3.3	Remote Access Record Flag	18
6.3.3.4	Remote Access Date Flag (immediate).....	18
6.3.3.5	Remote Access Date Field	19
6.3.4	Proximity-based Propagation Control.....	19
6.3.4.1	Local Movement and Copying Enabled (MLocal).....	19
6.3.4.2	Local Viewing Enabled (VLocal)	19
6.4	Output Control.....	19
6.4.1	Controlled Export/Output	19
6.4.1.1	Export/Output Control to Controlled CPS	19
6.4.1.2	Controlled CPS Vector.....	20
6.4.2	Untrusted Export.....	20
6.4.3	Disable Analogue SD Export.....	20
6.4.4	Disable Analogue SD Consumption	20
6.4.5	Disable Analogue HD Export	20
6.4.6	Disable Analogue HD Consumption.....	20
6.4.7	Image Constraint.....	21
6.5	Ancillary Control.....	21
6.5.1	Do Not CPCM Scramble (DNCS)	21
7	CPCM Auxiliary Data.....	21
7.1	General	21
7.2	CPCM Auxiliary Data for Original USI Maintenance	22
7.3	CPCM Auxiliary Data for Geographic Area Definition.....	22
7.4	CPCM Auxiliary Data for Export/Output to Trusted CPS	22
7.5	CPCM Auxiliary Data for Export/Output to Controlled CPS	22
7.6	CPCM Auxiliary Data for Analogue Protection Systems	22
8	Syntax of USI and CPCM Auxiliary Data	23
8.1	CPCM USI Syntax	23
8.2	CPCM Auxiliary Data Syntax.....	24
History	28

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).

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 3 of a multi-part deliverable. Full details of the entire series can be found in part 1 [1].

Introduction

CPCM is a system for Content Protection and Copy Management of commercial digital content delivered to consumer products. CPCM manages content usage from acquisition into the CPCM system until final consumption, or export from the CPCM system, in accordance with the particular usage rules of that content. Possible sources for commercial digital content include broadcast (e.g. cable, satellite, and terrestrial), Internet-based services, packaged media, and mobile services, among others. CPCM is intended for use in protecting all types of content - audio, video and associated applications and data. CPCM specifications facilitate interoperability of such content after acquisition into CPCM by networked consumer devices for both home networking and remote access.

This first phase of the specification addresses CPCM for digital Content encoded and transported by linear transport systems in accordance with TS 101 154 [i.1]. A later second phase will address CPCM for Content encoded and transported by systems that are based upon Internet Protocols in accordance with TS 102 005 [i.2].

1 Scope

The present document specifies the Usage State Information (USI) for the Digital Video Broadcasting (DVB) Content Protection and Copy Management (CPCM) system. Additionally, the present document specifies USI-related Auxiliary Data that will be carried along with the USI by mechanisms to be specified further by CPCM.

NOTE: USI has been designed to accommodate a variety of business models and regulatory regimes. The existence of any particular field of USI does not imply that it will be asserted by a particular business or that it will be allowed to be asserted.

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 102 825-1: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 1: CPCM Abbreviations, Definitions and Terms".
- [2] ETSI TS 102 825-4: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 4: CPCM System Specification".
- [3] ETSI TS 102 825-9: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 9: CPCM System Adaptation Layers".
- [4] ETSI TS 102 825-10: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 10: CPCM Acquisition, Consumption and Export Mappings".
- [5] ETSI TS 102 825-2: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 2: CPCM Reference Model".

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 101 154: "Digital Video Broadcasting (DVB); Specification for the use of Video and Audio Coding in Broadcasting Applications based on the MPEG-2 Transport Stream".
- [i.2] ETSI TS 102 005: "Digital Video Broadcasting (DVB); Specification for the use of Video and Audio Coding in DVB services delivered directly over IP protocols".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 102 825-1 [1] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TS 102 825-1 [1] apply.

4 Usage State Information General Requirements

4.1 Definition and application

The DVB CPCM Usage States Information (USI) is CPCM Content metadata that signals the Authorized Usage for that particular Content Item.

Authorized Usage is the permitted usage of CPCM Content, consisting of the set of Usage Rules applied to that Content.

Content is data that is to be protected by the CPCM System. This is generally audio-visual content plus optional accompanying data, such as subtitles, images/graphics, animations, web pages, text, games, software (both source code and object code), scripts or any other information which is intended to be delivered to and consumed by a user.

Usage Rules are the particular operations or behaviours that are within the scope of Content Protection and Copy Management and are to be controlled by the CPCM System through CPCM specifications and C&R regime.

NOTE 1: Usage Rules are established in the context of Usage Rights that exist or are granted on a per-Content Item basis. Usage Rights are explicit privileges, granted by the Rights Holder of the Content, to perform a particular operation on that Content. A Rights Holder is a person or entity that owns copyright or holds legitimate distribution rights to a particular Content Item.

NOTE 2: The possible set of Usage Rights will be established by the capabilities of a compliant CPCM system and therefore will be in accordance with both the CPCM specifications and C&R regime.

4.2 CPCM Content Licence

The USI is contained within a higher level DVB CPCM metadata structure called the CPCM Content Licence. The CPCM Content Licence is generated upon Acquisition. The CPCM Content Licence shall include the following fields as defined in TS 102 825-4 [2] some of which may not be systematically populated:

- Content Licence Version Information.
- Content Licence Identifier (CLID).
- Content Licence Creator (CLC).
- C&R regime information.
- Revocation information.
- Authorized Domain Identifier (ADID).
- Content Descrambling Information.
- Usage State Information (USI).

- Content Licence Management Data.

4.3 Secure Binding to Content

The USI of a given Content Item shall be securely bound to its Content Item, i.e. they shall be inextricably linked and no other USI shall be able to be substituted for it except as specifically permitted by compliant behaviour.

4.4 Content Entering DVB CPCM System

When Content first enters the DVB CPCM system, at a particular Acquisition Point, the Authorized Usage of that Content shall be determined and then preserved by securely binding it as USI metadata to the Content.

The DVB CPCM System shall only Acquire content for which there is an approved Usage Rule mapping, i.e. from a Trusted Source that includes Usage Rule signalling known to and trusted by DVB CPCM as set forth in a future C&R regime for DVB CPCM and/or other DVB specifications.

When Acquiring Content, if all, or some portion, of the information associated with an item of content that would be used to determine a trusted Usage Rule mapping is found to be corrupted or unintelligible due to errors, the appropriate Usage Rule shall be deemed to be the most restrictive states of contextually applicable USI for that portion of the information that is in question due to those errors.

NOTE: The Authorized Usage of Acquired Content might be determined through a variety of mechanisms. Among the more simple might be the static mapping of a single flag to a static, predetermined set of USI fields at the Acquisition Point. Among the more complex might be the interaction of an importing Conditional Access (CA) or Digital Rights Management (DRM) system authorized agent handling the commercial transactions associated with flexible content delivery business models with the DVB CPCM system through the Acquisition Point. In the latter case, an importing CA/DRM system maps from a large number of possibilities (full set of pre-Acquisition offerings) to a specific set of USI (post-Acquisition usages allowed within, e.g. a home network and/or beyond a home network). Moreover, there are situations where the Content Licence may be re-Acquired (hence, re-mapped) at a later stage, by the Rights Holder as identified in the Content Licence, through the Acquisition Point, conditional to a commercial transaction controlled by the Rights Holder associated with the importing CA/DRM and therefore beyond the scope of DVB CPCM; e.g. if the resulting CPCM USI are constrained over time (e.g. rental window).

4.5 Content within DVB CPCM System

In the case of a transfer of Content from one DVB CPCM Instance to another DVB CPCM Instance, all of the USI shall be securely conveyed and shall remain securely bound to the Content.

Certain USI fields may change through a secure process, for example:

- transition from Copy Once to Copy No More;
- transition from Zero Retention not asserted to Zero Retention asserted;
- modification of a USI field by the Rights Holder as defined in clause 4.1, such modification to be performed through a Content Licence re-Acquisition by an Authorized Authenticated Agent; and
- transition from VPA asserted to VPA not asserted upon first Consumption of Content and modification of VWA and View Window accordingly.

Changes to USI fields are only permitted under circumstances defined in CPCM System specifications (TS 102 825-4 [2]). The conditions and mechanisms by which these changes occur are beyond the scope of the present document.

4.6 Propagation Controls

The DVB CPCM USI includes a variety of propagation USI that enable Copying, Movement and Viewing of Content within defined groups of DVB CPCM compliant devices. Copying and Movement are controlled together and use the same USI fields. Viewing, or Consumption, can be controlled independently and therefore uses separate USI fields. These USI fields are specified in detail in the following clauses. This clause provides an overview of the logical and physical groups of devices and the hierarchical, precedence and transitional relationships between the various groups of devices.

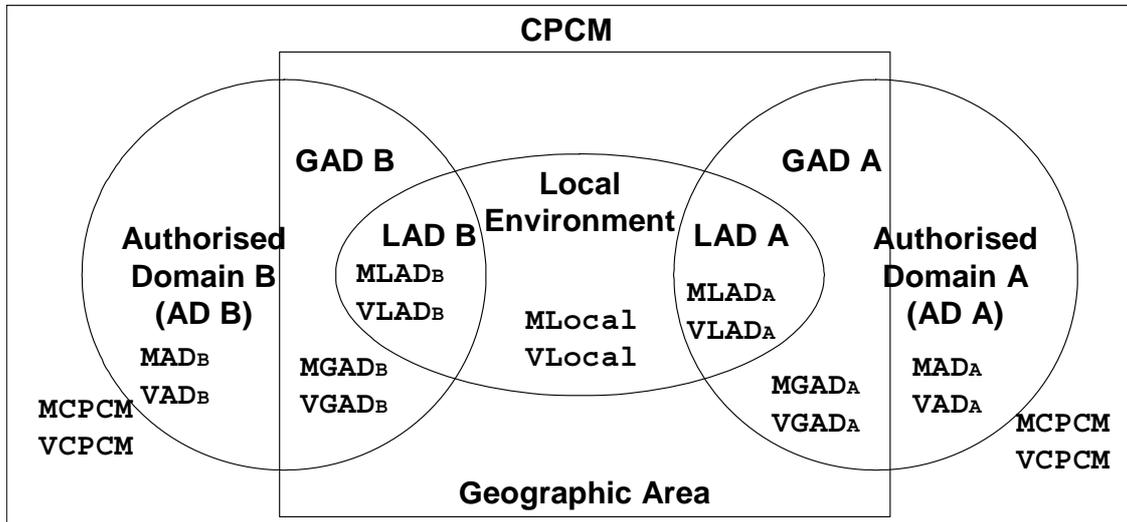


Figure 1: USI to Manage Content within CPCM Device Groups

Table 1: Key for USI to Manage Content within CPCM Device Groups

Key
USI nomenclature
"M" is a prefix for Copying and Movement control; "V" is a prefix for Consumption/Viewing Control; and the area in which that M and/or V usage is specified is the group of CPCM Devices denoted by the remainder of the USI field name, i.e. "CPCM", "AD", "GAD", "LAD" and/or "Local".
Sets of CPCM Devices that can be granted usage, as a group, through USI settings
CPCM = the total set of CPCM compliant devices => the outer box AD = Authorized Domain => two circular areas, AD A and AD B. GAD = Geographically-constrained AD (i.e. in the same AD and in the same Geographic Area) => two semi-circular areas, GAD A and GAD B. LAD = Localized AD => intersection of their respective ADs circles and the LE ellipse, LAD A and LAD B. "Local" or LE => Local Environment => ellipse
Transition
LAD (or GAD) is not a permanent restriction. The usage permission for LAD and GAD transitions to the entire AD, after the Remote Access Rule is satisfied.
Proximity-dependent (and AD-independent) local usage
MLocal and VLocal are independent of AD-related controls and only dependent on proximity-related controls. If MCPDM or VCPCM is allowed, then MLocal or VLocal, respectively, is redundant.

A hierarchical relationship between groups of CPCM Devices that are members of an AD is depicted in Figure 1. The hierarchy, from broadest to most narrow, is as follows:

- The collection of all CPCM Devices located anywhere in the world - the outer white box (signalled by MCPDM and VCPCM USI).
- The Authorized Domain (AD) - all CPCM Devices that are members of the same AD and located anywhere in the world (signalled by MAD and VAD USI).
- The Geographically-constrained AD (GAD) - all CPCM Devices that are members of the same AD that are located in the same Geographic Area (signalled by MGAD and VGAD USI).

- d) The Localized AD (LAD) - all CPCM Devices that are members of the same AD that are in the same Local Environment, e.g. in the same home or car (signalled by MLAD and VLAD USI).

Therefore, for Devices that are members of an AD:

- MLAD, MGAD, MAD and MCPCM are the different possible states of the Movement and Copying Propagation Information field, progressing from the narrowest to the broadest.
- VLAD, VGAD, VAD and VCPCM are the different possible states of the Viewing Propagation Information field, progressing from the narrowest to the broadest.

Additionally, the Local Environment logical construct is used orthogonal to the Authorized Domain and therefore has its own USI, MLocal and VLocal, to enable Local usage with respect to that logical construct. Note that if Movement and Copying is allowed by any CPCM Device by the assertion of MCPCM, then the assertion of MLocal is redundant and adds no further breadth of usage. Likewise, if Viewing is allowed by any CPCM Device by the assertion of VCPCM, then the assertion of VLocal is redundant and adds no further breadth of usage. So "Local" and "CPCM" also have a hierarchical relationship, independent of AD membership.

There is a transitional relationship between a Localized AD and an AD. Content for which usage is allowed only within the LAD will, upon fulfilment of a condition defined in the Remote Access Rule USI, transition to a state that allows usage within the entire AD. Likewise, if usage is restricted to the GAD, the GAD usage permission will transition to AD usage permission upon fulfilment of the Remote Access Rule.

The following informative examples will help illustrate the relationships. In one example, Content could be delivered to a Singaporean home via a satellite subscription television receiver (an Acquisition Point) for use by any Device on the home network (LAD), then after 24 hours (a possible Remote Access Rule condition), be accessed by a remote TV (Consumption Point) in the same user's portable device while he is travelling in Hawaii (another Device in the same AD).

In another variation of the same example, the Content may be delivered with USI allowing immediate usage in the same AD but restricted to Singapore for the first 24 hours followed by remote access anywhere in the world within the same AD. This content would have MGAD and VGAD asserted with a geographic area defined as "Singapore". During the first 24 hours after reception, any portable devices within the same AD that are located within Singapore would be able to access the content. After the first 24 hours elapses, it would not matter if a Device was in Singapore or not since only the AD membership would matter. A CPCM Device may use the tools that are used to control LAD usage in order to inherently fulfil a GAD restriction, e.g. if Content does not leave the Singaporean home, then it follows that it has not left Singapore.

In a third example, the Content in either of the previous two examples could also be marked with USI that allowed usage within the Local Environment. If that were the case, then in addition to the allowed usages described above, Content could be Copied or Moved (controlled by MLocal) or Consumed/Viewed (controlled by VLocal) by any CPCM Device, regardless of AD membership, that was located in the same Local Environment, e.g. the same Singaporean home.

In each example above, the Copy and Movement controls are set to the same state as the Viewing controls. These could be set differently, for example, to enable immediate Copying and Movement within the GAD and Viewing within the entire AD. Then after, for example, 24 hours, Copying, Movement and Viewing could all be enabled in the entire AD.

The broadest level of redistribution-related usage that can be signalled by CPCM USI is a state that allows redistribution of Content to any compliant DVB CPCM Device. This area is depicted in Figure 1 by the white box that includes all other items. If content was Acquired by a device in AD_A and Copying and Movement was not restricted to that Authorized Domain then the Content would be marked MCPCM. If viewing, likewise, was not restricted to that AD, then the Content would be marked VCPCM. The same applies to Content Acquired by a Device that is a member of AD B. Content marked MCPCM can be Copied and/or Moved to the collection of all CPCM Devices located anywhere in the world. Content marked VCPCM can be Viewed/Consumed by the collection of all CPCM Devices located anywhere in the world.

4.7 Content Exported/Output from the CPCM System to a Trusted or Controlled CPS

Content can leave the CPCM System and go to another Trusted Content Protection System (CPS) through four different means that are described in TS 102 825-2 [5]:

- Export of Content to a Controlled CPS.
- Export of Content to a Trusted CPS.
- Output of Content via a digital Consumption Output to a Controlled CPS.
- Output of Content via a digital Consumption Output to a Trusted CPS.

A Controlled CPS is a Trusted CPS to which Export or Output can be enabled and disabled subject to specific USI. In any of these four means of Content leaving CPCM, the USI shall be mapped to a predefined state of usage state information within that Trusted CPS or Controlled CPS. Export/Output to a Trusted CPS is not governed by a dedicated USI field but by a C&R regime while Export/Output to Controlled CPS is governed by both a dedicated USI field and the relevant C&R regime.

NOTE: Identification of the Trusted and Controlled CPSs and specification of their respective USI mappings are beyond the scope of this multi-part deliverable.

4.8 Content Exported from the CPCM System to an Untrusted Space

Content can be Exported to an Untrusted Space if so signalled. An Untrusted Space is any system, entity, device, component, medium, function, interface or any other tangible or intangible thing other than the CPCM System, all Trusted CPSs and all Controlled CPSs.

There may still be Authorized Usage required for such content, e.g. "private use only" and "not for resale", but enforcement of these rights will not be managed by the tools and systems of DVB CPCM or a Trusted or Controlled CPS once content has been so Exported.

4.9 Extensions

The CPCM baseline functionality may be extended where necessary for particular proprietary functionality, or for future additional extended CPCM functionality. This shall be done as described in the CPCM Extension section of TS 102 825-2 [5]. The CPCM System includes the facility for data for extended CPCM functionality to be carried in the Content Licence (CL) and/or by other mechanisms. This data may be, for example, Extended USI or Extended Auxiliary Data. Detailed definition of this data is beyond the scope of this multi-part deliverable.

NOTE: The description of extensions for proprietary functionalities is beyond the scope of this multi-part deliverable.

5 Overview of USI Fields

Table 2: Usage State Information Overview

USI field name	Meaning (short version)
Copy and Movement Control - see clause 6.1	
Copy Control Information (CCI)	The Copy Control Information field that has four states: CCNA, C1, CNM, or CN.
CCNA	"Copy Control Not Asserted" state of CCI.
C1	"Copy Once" state of CCI.
CNM	"Copy No More" state of CCI.
CN - Zero Retention not Asserted	"Copy Never" state of CCI. Content may be temporarily stored or retained for the purpose of enabling pause or trick modes
CN - Zero Retention Asserted	"Copy Never" state of CCI. Content shall not be temporarily stored or retained for the purpose of enabling pause or trick modes
Consumption Control - see clause 6.2	
Viewable (V)	Viewing, i.e. Consumption, is enabled.
View Window Activated (VWA)	Viewing, i.e. Consumption, is limited by the View Window field.
View Window	An absolute period of time specified using an absolute start time and an absolute end time.
View Period Activated (VPA)	Viewing, i.e. Consumption, is limited by the View Period From First Playback field.
View Period From 1 st Playback	A period of time relative to first Consumption of live input Content or first playback of a stored Copy not previously Consumed.
Simultaneous View Count Activated (SVCA)	Simultaneous Viewing, i.e. Consumption, is numerically limited.
Simultaneous View Count	If SVCA is asserted, this field indicates the number of concurrent Consumption Points Export Points that can be used for the Live/Direct Consumption and Export of a Content Item.
Propagation Control - see clause 6.3	
Movement and Copying Propagation Information	The Movement and Copying Propagation Information field that has four states: MLAD, MGAD, MAD or MCPCM.
MLAD	Copying and/or Movement within the same Localized AD is allowed.
MGAD	Copying and/or Movement within the same Geographically-constrained AD is allowed.
MAD	Copying and/or Movement within the same Authorized Domain is allowed.
MCPCM	Copying and/or Movement to any CPCM-compliant Storage Entity is allowed.
Viewing Propagation Information	The Viewing Propagation Information field that has four states: VLAD, VGAD, VAD or VCPCM.
VLAD	Viewing, i.e. Consumption, within the same Localized AD is allowed.
VGAD	Viewing, i.e. Consumption, within the same Geographically-constrained AD is allowed.
VAD	Viewing, i.e. Consumption, within the same Authorized Domain is allowed.
VCPCM	Viewing, i.e. Consumption, using any CPCM-compliant Consumption Point is allowed.
Remote Access Rule	These fields define the conditions under which Copying, Movement and/or Consumption shall transition from being allowed only within the Localized AD, or Geographically-constrained AD, to being allowed in the entire AD.
MLocal	Copying and/or Movement is allowed if the Destination is Local to the Source, e.g. both within the same home.
VLocal	Viewing, i.e. Consumption, is allowed if the Consumption Point is Local to the Source, e.g. both within the same home.
Output Control - see clause 6.4	
Export/Output Controlled CPS	Content may be exported or output to Controlled CPSs defined in the Controlled CPS Vector.
Controlled CPS Vector	A vector that identifies Controlled CPSs to which Export/Output is allowed.
Export Beyond Trust	Content may be Exported to an Untrusted Space.
Disable Analogue SD Export	Export of standard definition analogue content is prohibited.
Disable Analogue SD Consumption	Output of standard definition analogue content for consumption is prohibited.
Disable Analogue HD Export	Export of high definition analogue content is prohibited.
Disable Analogue HD Consumption	Output of high definition analogue content for consumption is prohibited.
Image Constraint	Constrain image resolution of high definition analogue outputs and Export to an Untrusted Space.
Ancillary Control - see clause 6.5	
Do Not CPCM Scramble	Content shall not be scrambled by the CPCM Scrambler.

6 Detailed Description of USI Fields

The syntax given in this clause and in the following clause is mandatory.

6.1 Copy and Movement Control

6.1.1 Copy Control Information (CCI)

The Copy Control Information field can take on four states:

- CCNA;
- C1;
- CNM; or
- CN.

6.1.2 Copy Control Not Asserted (CCNA)

"Copy Control Not Asserted" is a Copy Control Information state that means that the Authorized Usage shall not include numerical restrictions to Copying.

6.1.3 Copy Once (C1)

"Copy Once" is a Copy Control Information state that means that the Authorized Usage shall permit exactly one Copy. The resulting Copy is marked "Copy No More".

"Copy Once" can only apply to "live" Content (i.e. contemporaneous to the Content's Acquisition), since any stored Copy must be remarked "Copy No More".

NOTE: The CPCM USI uses the "Copy Once" state. Some other content protection systems use a CCI state of "Copy One Generation". The precise mapping between these systems is beyond the scope of this multi-part deliverable.

6.1.4 Copy No More (CNM)

"Copy No More" is a Copy Control Information state that means that the Authorized Usage shall not permit Copying. This Copy Control Information state is given to Copies of "Copy Once" Content during the Copying process.

NOTE: Content that is marked "Copy No More" is Movable. Moving is the process of making a Copy wherein the original is then removed, erased or made no longer accessible. In practice it may not be possible to "Move" content from certain types of write once media, while it may, of course, be possible to "physically move" the media.

6.1.5 Copy Never (CN) Zero Retention Not Asserted

"Copy Never" is a Copy Control Information state that means that the Authorized Usage shall not permit Copying.

Further storage or buffering of "Copy Never" content is allowed to facilitate a fixed time period pause and trick mode function, e.g. because such capability is not otherwise available to the user via an upstream Source of this Content. The allowed fixed time period for storage or buffering will be defined by the C&R regime.

If Content that is marked "Copy Never" zero_retention not asserted is buffered; e.g. for the purpose of enabling pause or trick modes, then the Content output from the Storage Entity used to buffer the Content shall be remarked with "Copy Never" with zero_retention asserted.

6.1.6 Copy Never (CN) Zero Retention Asserted

If zero_retention is asserted, then Content with a CCI state of "Copy Never" shall not be stored or retained for the purpose of enabling pause or trick modes.

zero_retention is provided to indicate that no further storage or buffering of "Copy Never" content is allowed to facilitate a fixed time period pause and trick mode function, e.g. because such capability is available to the user via an upstream Source of this Content.

6.2 Consumption Control

6.2.1 Viewable (V)

If V is asserted, viewing, i.e. Consumption or Export, is enabled, subject further to the View Window and the View Period.

If V is not asserted then Consumption and Export are not enabled.

NOTE: Content may be Acquired into CPCM with V not asserted; this allows the Content to be managed by CPCM prior to authorization to Consume or Export.

In order for Consumption or Export to be enabled:

- a) V must be asserted;
- b) the View Window must be open if VWA is asserted;
- c) the View Period must not have expired if VPA is asserted; and
- d) the simultaneous_view_count, if SVCA is asserted, has not been exceeded.

6.2.2 View Window

6.2.2.1 View Window Activated (VWA)

If VWA is asserted, viewing, i.e. Consumption or Export, is temporally limited by the View Window field, i.e. Consumption is:

- a) enabled when the View Window is enabled, or open, subject further to the V field and the View Period; and
- b) disabled when the View Window is not enabled, or closed.

If VWA is not asserted, Consumption and Export are not temporally limited by the View Window field.

NOTE 1: The View Window defines when Consumption or Export is enabled and when it expires in terms of an absolute start time (view_window_start) and an absolute end time (view_window_end).

NOTE 2: Unless the view_window_start precedes the view_window_end, the View Window can never be enabled, or open.

6.2.2.2 View Window Start

The view_window_start field defines the start time upon which the View Window is enabled, or opened. It is defined as absolute start time.

The format of this field is defined in CPCM Systems Specification (TS 102 825-4 [2]).

6.2.2.3 View Window End

The `view_window_end` field defines the end time after which the View Window is disabled, or closed. It is defined as absolute expiry time.

The format of this field is defined in CPCM Systems Specification (TS 102 825-4 [2]).

6.2.3 View Period

6.2.3.1 View Period Activated (VPA)

If VPA is asserted, viewing, i.e. Consumption or Export, is enabled for a limited period of time after first playback of the Content, the View Period, as specified by the `view_period_from_first_playback` field, subject further to the V field and the View Window.

If VPA is asserted and the `view_period_from_first_playback` has expired, then Consumption and Export are not enabled.

If VPA is not asserted, Consumption is not temporally limited by the `view_period_from_first_playback` field.

NOTE: Upon first Consumption or Export, VPA will be unasserted and VWA and View Window fields updated to achieve the equivalent usage defined by VPA and View Period fields.

6.2.3.2 View Period From First Playback

The `view_period_from_first_playback` field defines when Consumption or Export is enabled and when it expires in terms of a period of time relative to first Consumption or Export of a stored Copy (or first Consumption or Export of live Input Content that is stored for additional future Consumption). The right to Consume or Export the Content Item shall expire `view_period_from_first_playback` after first Consumption or Export of the live Input Content or after first playback of a Copy that was not Consumed or Exported when first Acquired.

The `view_period_from_first_playback` is coded as a 16-bit field that defines a number of 15-minute intervals. The value 0x0000 is zero minutes. The value 0xFFFF is approximately 1,87 years.

Before the first Consumption or Export, the Content may be stored in only one location. If the user wants to make a Copy of that content, it shall either be not accepted or it be accepted but be considered equivalently to a Consumption or Export.

6.2.4 Simultaneous View Count

6.2.4.1 Simultaneous View Count Activated (SVCA)

If SVCA is asserted, then viewing, i.e. simultaneous Consumption and Export, is numerically limited.

If SVCA is not asserted, then viewing, i.e. simultaneous Consumption and Export, is not numerically limited.

NOTE: See the `simultaneous_view_count` below for another means to "not assert" SVCA.

6.2.4.2 Simultaneous View Count

The `simultaneous_view_count` field indicates the number of concurrent Consumption Points and Export Points that can be used for the Live/Direct Consumption and Export of a Content Item. The eight-bit `simultaneous_view_count` field is defined in Table 3.

Table 3: Simultaneous View Count Description

Value	Meaning
0	Condition not asserted. Equivalent to not asserting SVCA.
1 to 255	Maximum permitted number of concurrent Consumes and Exports.

If SVCA is asserted, then the sum of all concurrent Consumes and Exports must be less than or equal to `simultaneous_view_count`.

EXAMPLE: If SVCA is asserted and the count is set to four, then an attempt to enable viewing on a fifth display will fail. Such a capability might be used in a PayTV environment that limits the number of active allowed consumption devices in a home account that makes use of CPCM devices.

6.3 Propagation Control

6.3.1 Movement and Copying Propagation Information

The Movement and Copying Propagation Information can take on four states: MLAD, MGAD, MAD or MCPCM. See clause 4.6 for a description of propagation controls.

6.3.1.1 Movement and Copying Within Localized AD Enabled (MLAD)

If asserted, Copying and/or Movement to another Storage Entity (or via a CPCM Device) is allowed within the same Localized AD, subject to the states of the CCI field.

NOTE: This is the minimum extent of Propagation that can be signalled by the Movement and Copying Propagation Information.

6.3.1.2 Movement and Copying Within GAD Enabled (MGAD)

If asserted, Copying and/or Movement to another Storage Entity (or via a CPCM Device) is allowed within the same Geographically-constrained AD (GAD), subject to the states of the CCI field. The GAD is the AD constrained to the Geographic Area specified in an Auxiliary Data field described in clause 7.2.

NOTE 1: The MGAD state is only useful for devices with explicit knowledge of their geographical location, an optional functionality of DVB CPCM. Devices that do not have this ability would instead allow MLAD usage which is inherently compliant with MGAD usage. Additionally, any CPCM Device may use the LAD tools to control MGAD usage in order to inherently fulfil an MGAD restriction.

NOTE 2: If MGAD is asserted, Movement and Copying within the LAD is always permitted subject to the states of the CCI field.

6.3.1.3 Movement and Copying Within AD Enabled (MAD)

If asserted, Copying and/or Movement to another Storage Entity (or via a CPCM Device) is allowed within the same Authorized Domain, subject to the states of the CCI field.

If MLAD or MGAD is asserted, then the same Authorized Usage that is allowed by MAD shall be allowed upon fulfilment of conditions specified in the Remote Access Rule.

6.3.1.4 Movement and Copying Within CPCM Enabled (MCPCM)

If asserted, Copying and/or Movement to any CPCM-compliant Storage Entity (or via any CPCM Device) is allowed, subject to the states of the CCI field.

6.3.2 Viewing Propagation Information

The Viewing Propagation Information can take on four states: VLAD, VGAD, VAD or VCPCM. See clause 4.5 for a description of propagation controls.

NOTE: It may not make sense to assert more restrictive propagation control on Viewing (Consumption) than on Movement and Copying since the equivalent functionality could be obtained by first Moving a Copy and then Viewing that Copy. Accordingly, the anticipated usage of Viewing Propagation Information is to allow equal or greater breadth of propagation for the Viewing function than for Copying and Movement.

6.3.2.1 Viewing Within Localized AD Enabled (VLAD)

If asserted, viewing, i.e. Consumption, is allowed using a Consumption Point (or via a CPCM Device) in the same Localized AD, subject to the states the V, VWA, View Window, SVCA and simultaneous_view_count fields.

NOTE: This is the minimum extent of Propagation that can be signalled by the Viewing Propagation Information.

6.3.2.2 Viewing Within GAD Enabled (VGAD)

If asserted, viewing, i.e. Consumption, is allowed using a Consumption Point (or via a CPCM Device) in the same Geographically-constrained AD, subject to the states of the V, VWA, View Window, SVCA and simultaneous_view_count fields. The GAD is the AD constrained to the Geographic Area specified in a Content Licence Auxiliary field described in clause 7.2.

NOTE 1: The VGAD state is only useful for devices with explicit knowledge of their geographical location, an optional functionality of DVB CPCM. Devices that do not have this ability would instead allow VLAD usage which is inherently compliant with VGAD usage. Additionally, any CPCM Device may use the LAD tools to control VGAD usage in order to inherently fulfil a VGAD restriction.

NOTE 2: If VGAD is asserted, viewing, i.e. Consumption within the LAD is always permitted subject to the states the V, VWA, View Window, SVCA and simultaneous_view_count fields.

6.3.2.3 Viewing Within AD Enabled (VAD)

If asserted, viewing, i.e. Consumption, is allowed using a Consumption Point (or via a CPCM Device) in the same Authorized Domain as the Content Source, subject to the states of the V, VWA, View Window, SVCA and simultaneous_view_count fields.

If VLAD or VGAD is asserted, then the same Authorized Usage that is allowed by VAD shall be allowed upon fulfilment of conditions specified in the Remote Access Rule.

6.3.2.4 Viewing Within CPCM Enabled (VCPCM)

If asserted, viewing, i.e. Consumption, is allowed using any CPCM-compliant Consumption Point, subject to the states of the V, VWA, View Window, SVCA and simultaneous_view_count fields.

6.3.3 Transition from "LAD or GAD Usage" to "AD Usage"

6.3.3.1 Remote Access Rule

The Remote Access Rule defines the conditions under which Copying, Movement and/or Consumption shall transition from being allowed only within the Localized AD or Geographically-constrained AD to being allowed within the entire AD, i.e. "Remote Access" within an AD. It therefore has meaning with respect to Copying and Movement if MAD is not asserted and instead MLAD or MGAD is asserted. It likewise has meaning with respect to Viewing if VAD is not asserted and instead VLAD or VGAD is asserted.

Remote Access Rule shall be a logical combination of the flags and fields shown in Table 4.

Table 4: Remote Access Rule Components

Field	Meaning
remote_access_date_moving_window_flag remote_access_date	A flag and field that can be used to allow Remote Access a specified period of time after Acquisition of the Content Item. After this date and time, content item will be available for Remote Access on the basis of a real-time moving window i.e. the beginning of the Content Item is available at this date and time and the end of the Content Item is available at this date and time plus the duration of the Content Item.
remote_access_record	A flag that can be used to allow Remote Access after recording of a Content Item is completed.
remote_access_date_immediate_flag remote_access_date	A flag and field that can be used to allow Remote Access of a Content Item commencing on a specified date and time. Entire Content Item is immediately available after this date and time.

If one flag in the Remote Access Rule is asserted then Remote Access can commence upon that asserted condition becoming true and continue in accordance with other USI.

If none of the three flags are asserted then Remote Access can commence immediately in accordance with other USI fields.

If more than one flag in the Remote Access Rule is asserted then Remote Access can commence upon any one of those asserted conditions becoming true and continue in accordance with other USI.

6.3.3.2 Remote Access Date flag (moving window)

If remote_access_date_moving_window_flag is asserted then Remote Access is allowed for a specific part of the Content Item, in accordance with other USI fields, starting when the absolute date specified in the remote_access_date Field augmented with the time duration elapsed between the beginning of the Content and the Content Item matches the current date.

If remote_access_date_immediate_flag and remote_access_date_moving_window_flag are asserted, less restrictive usage shall be applied and only remote_access_date_immediate_flag is considered.

This flag is expected to be mapped from the broadcast USI signal remote_access_delay_flag. Upon receipt of such USI, the Acquisition Point sets remote_access_date_moving_window_flag and sets remote_access_date Field to the current Date augmented with the remote_access_delay field. If remote_access_date Field is already set, the Acquisition Point shall set this field to the minimum of the two values. If minimum corresponds to remote_access_date_moving_window_flag, remote_access_date_immediate window_flag shall be unasserted.

6.3.3.3 Remote Access Record Flag

If the remote_access_record flag is asserted then Remote Access is allowed, in accordance with other USI fields, upon the end of recording of the particular Content Item.

The format of this field is defined in CPCM Systems Specification (TS 102 825-4 [2]).

6.3.3.4 Remote Access Date Flag (immediate)

If the remote_access_date_immediate_flag is asserted then Remote Access of the entire Content Item is allowed, in accordance with other USI fields, starting when the absolute date specified in the remote_access_date Field matches the current date.

6.3.3.5 Remote Access Date Field

The `remote_access_date` field specifies an absolute date and time after which Remote Access to Content is enabled. Remote Access can be enabled immediately for whole Content or on a moving window basis.

Table 5: Interpretation of `remote_access_date`

<code>..._date_immediate_flag</code>	<code>..._moving_window_flag</code>	<code>remote_access_date</code> interpretation
0	0	Not applicable since not present
0	1	Moving window
1	0	Immediate
1	1	Immediate, since more permissive

6.3.4 Proximity-based Propagation Control

6.3.4.1 Local Movement and Copying Enabled (MLocal)

If asserted, Moving and/or Copying to another Storage Entity (or via a CPCM Device) is allowed if the Destination is Local to the Source, e.g. both within the same home, subject to the states of the CCI field.

If not asserted, then this field carries no meaning and Movement and Copying Propagation is controlled exclusively by Movement and Copying Propagation Information.

NOTE 1: The assertion of MLocal allows local copies to be made or copies to be moved without regard to AD membership.

NOTE 2: If Movement and Copying is allowed by any CPCM Device by the assertion of MCPCM, then the assertion of MLocal is redundant because it does not modify the breadth of usage.

6.3.4.2 Local Viewing Enabled (VLocal)

If asserted, viewing, i.e. Consumption, using a Consumption Point (or via a CPCM Device) is allowed, if the Consumption Point (or CPCM Device) is Local to the Source, e.g. both within the same home, subject to the states of the V, VWA, View Window, SVCA and `simultaneous_view_count` fields.

If not asserted, then this field carries no meaning and Viewing Propagation is controlled exclusively by Viewing Propagation Information.

NOTE 1: The assertion of VLocal allows local viewing without regard to AD membership of the Consumption Point.

NOTE 2: If Viewing is allowed by any CPCM Device by the assertion of VCPCM, then the assertion of VLocal is redundant because it does not modify the breadth of usage.

6.4 Output Control

6.4.1 Controlled Export/Output

6.4.1.1 Export/Output Control to Controlled CPS

Controlled Export/Output is the digital output of CPCM Content mapped to a Controlled CPS under the explicit control of the USI of that CPCM Content. Such output is either:

- a) Export of Content to a Controlled CPS; or
- b) Output of Content via a digital Consumption Output to a Controlled CPS. If `export/output_controlled_CPS` is asserted, Content may be Exported or Output in accordance with the USI mapping beyond the CPCM System to any Controlled CPS identified in the Controlled CPS Vector.

NOTE 1: A Controlled CPS is a Trusted CPS to which Export can be enabled or disabled subject to USI. A Trusted CPS is a trusted, third-party content protection system with which a predetermined set of CPCM interoperability rules, including a USI mapping, has been defined and approved by the authority responsible for a particular CPCM C&R regime. The mechanisms and entities required for approval of such a Controlled CPS and the USI mapping are beyond the scope of this multi-part deliverable.

NOTE 2: There is no USI to control Export/Output of Content to a Trusted CPS (that is not also a Controlled CPS). Export/Output to a Trusted CPS is not governed by a dedicated USI field but by a C&R regime while Export/Output to Controlled CPS is governed by both a dedicated USI field and the relevant C&R regime.

6.4.1.2 Controlled CPS Vector

The `controlled_CPS_vector` identifies Controlled CPSs to which Export or Output is allowed for a particular C&R regime.

6.4.2 Untrusted Export

If `export_beyond_trust` is asserted, Content may be Exported to an Untrusted Space.

If `export_beyond_trust` is not asserted, Content shall not be Exported to an Untrusted Space.

NOTE: An Untrusted Space is any system, entity, device, component, medium, function, interface or any other tangible or intangible thing other than the CPCM System, all Trusted CPSs and all Controlled CPSs.

6.4.3 Disable Analogue SD Export

If `disable_analogue_SD_export` is asserted, then Analogue Export of CPCM Content in Standard Definition analogue form is prohibited.

If `disable_analogue_SD_export` is not asserted, then Analogue Export of CPCM Content in Standard Definition analogue form is permitted.

6.4.4 Disable Analogue SD Consumption

If `disable_analogue_SD_consumption` is asserted, then Analogue Consumption Output of CPCM Content in Standard Definition analogue form is prohibited.

If `disable_analogue_SD_consumption` is not asserted, then Analogue Consumption Output of CPCM Content in Standard Definition analogue form is permitted.

6.4.5 Disable Analogue HD Export

If `disable_analogue_HD_export` is asserted, then Analogue Export of CPCM Content in High Definition analogue form is prohibited.

If `disable_analogue_HD_export` is not asserted, then Analogue Export of CPCM Content in High Definition analogue form is permitted.

6.4.6 Disable Analogue HD Consumption

If `disable_analogue_HD_consumption` is asserted, then Analogue Consumption Output of CPCM Content in High Definition analogue form is prohibited.

If `disable_analogue_HD_consumption` is not asserted, then Analogue Consumption Output of CPCM Content in High Definition analogue form is permitted.

6.4.7 Image Constraint

If `image_constraint` is asserted, then Content output to High Definition analogue Outputs or Content Exported to an Untrusted Space must first pass through a Processing operation that constrains the resolution of the image portion of the Content to a visual equivalent of no more than 520,000 pixels per frame (e.g. an image with resolution of 960 pixels by 540 pixels).

NOTE 1: For avoidance of any doubt, an image with horizontal resolution of 720 pixels and vertical resolution of 576 pixels fulfils the "no more than 520 000 pixels per frame" requirement.

NOTE 2: For avoidance of any doubt, `image_constraint` does not signal permitted scan rates or pixel structures used to generate analogue outputs.

NOTE 3: `image_constraint` may be attained through visual resolution reduction, e.g. by passing the Content through a Processing function that discards, dithers, or averages pixels to fulfil the requisite maximum visual resolution. The Processed video Content may then be displayed using other video Processing techniques such as line doubling or sharpening to improve the perceived quality of the image. By way of example, a Constrained Image may be stretched or doubled, and displayed full-screen, on a 1 080-line monitor. Alternatively, a 960 × 540 structure could be upconverted to 1 280 x 720 for output as a 720-line progressive signal.

6.5 Ancillary Control

6.5.1 Do Not CPCM Scramble (DNCS)

If DNCS is asserted, CPCM Content shall not be scrambled by the CPCM Scrambler.

If DNCS is not asserted, this field carries no meaning.

NOTE 1: The assertion of DNCS does not imply any relaxation of the enforcement of other associated USI; however, it is anticipated that DNCS may not be asserted with certain combinations of USI.

NOTE 2: This applies to any Acquired Content for which DNCS is asserted regardless of the source of the Content prior to Acquisition or the presence or absence of scrambling on that source signal.

7 CPCM Auxiliary Data

7.1 General

CPCM Auxiliary Data has the same general characteristics and requirements as USI:

- it is CPCM Content metadata that may be used along with USI to signal Authorized Usage for that particular Content Item;
- it is securely bound to the Content Item;
- it is determined and preserved upon Acquisition; and
- it may be used to determine a permitted mapping to a Trusted CPS or Controlled CPS.

Where the USI is a part of the Content Licence, CPCM Auxiliary Data may be too large to be contained within that structure. Therefore, CPCM Auxiliary Data shall be carried by other mechanisms. The method of carriage of Auxiliary Data is defined in TS 102 825-9 [3]. Content Licence Management Data include a secure link to CPCM Auxiliary Data that allows achieving the above requirements.

NOTE: The list of Auxiliary Data in this multi-part deliverable is not exhaustive. Other fields may be defined in other CPCM specifications.

7.2 CPCM Auxiliary Data for Original USI Maintenance

Within CPCM USI, some USI may change upon Content Usage (see clause 4.5). The goal of these auxiliary data is to maintain the original USI signalling upon Content Acquisition.

CPCM Auxiliary Data for Original USI maintenance can have two forms:

- Maintenance of original signalling associated with a Free-To-Air content.
- Maintenance of original USI as provided by the delivery system within the Acquisition Point.

7.3 CPCM Auxiliary Data for Geographic Area Definition

The Geographic Area in which propagation is allowed by MGAD and/or VGAD is carried in geographic_area data structure. The overall Geographic Area is expressed as up to 256 sets of geo_data structures, which allows multiple methods of encoding for same or similar areas. Propagation is allowed, in accordance with other USI, if the device can determine using at least one geo_data structure that it is within the specified area.

The geo_data structure, the coding methods and the geo data formats are defined in the System Specification (TS 102 825-4 [2]).

7.4 CPCM Auxiliary Data for Export/Output to Trusted CPS

A private data structure reserved for future use that may be used to carry, for example, data unique to each Trusted CPS.

Detailed definition of this data field and conditions for its use are:

- 1) beyond the scope of this multi-part deliverable;
- 2) may require further description in other DVB specifications and/or a C&R regime; and
- 3) may require harmonization with other standards organizations and private entities.

7.5 CPCM Auxiliary Data for Export/Output to Controlled CPS

A private data structure reserved for future use that may be used to carry, for example, data unique to each Controlled CPS.

- 1) Detailed definition of this data field and conditions for its use are defined by each C&R regime.

7.6 CPCM Auxiliary Data for Analogue Protection Systems

A private data structure to provide control signals to analogue output protection systems.

NOTE: Some Content may include this signalling to enable certain analogue protection systems on analogue outputs. At the time this multi-part deliverable was drafted, two different systems existed for standard definition outputs and none existed for high definition outputs. Additional standard definition systems and possible high definition systems may be defined in the future. This auxiliary data field provides a signalling path for both present and future systems.

Detailed definition of this Auxiliary Data field is beyond the scope of this multi-part deliverable.

8 Syntax of USI and CPCM Auxiliary Data

8.1 CPCM USI Syntax

Table 6 gives the syntax of CPCM USI.

Table 6: CPCM USI

Syntax	Bits	Identifier
CPCM_usage_state_information(){		
length	8	uimsbf
copy_control	3	uimsbf
do_not_cpcm_scramble	1	bslbf
viewable	1	bslbf
view_window_activated	1	bslbf
view_period_activated	1	bslbf
simultaneous_view_count_activated	1	bslbf
move_local	1	bslbf
view_local	1	bslbf
move_and_copy_propagation_information	2	uimsbf
view_propagation_information	2	uimsbf
remote_access_date_moving_window_flag	1	bslbf
remote_access_date_immediate_flag	1	bslbf
remote_access_record_flag	1	bslbf
export_controlled_cps	1	bslbf
export_beyond_trust	1	bslbf
disable_analogue_sd_export	1	bslbf
disable_analogue_sd_consumption	1	bslbf
disable_analogue_hd_export	1	bslbf
disable_analogue_hd_consumption	1	bslbf
image_constraint	1	bslbf
if (view_window_activated == 1){		
view_window_start	40	CPCM_date_time
view_window_end	40	CPCM_date_time
}		
if (view_period_activated == 1){		
view_period_from_first_playback	16	CPCM_playback_period
}		
if (simultaneous_view_count_activated == 1){		
simultaneous_view_count	8	uimsbf
}		
if (remote_access_date_immediate_flag == 1		
remote_access_moving_window_flag == 1){		
remote_access_date	40	CPCM_date_time
}		
if (export_controlled_cps == 1){		
cps_vector_count	8	
for (i=0; i<cps_vector_count; i++){		
C_and_R_regime_mask	8	
cps_vector_length	16	uimsbf
for (i=0; i<controlled_cps_length; i++){		
cps_vector_byte	8	bslbf
}		
}		
}		
}		
}		

Tables 7 to 9 further specify the syntax of Copy Control, Movement, Copying and Viewing Propagation Information.

Table 7: Copy Control

cci_and_zero_retention	Description
0	Copy Control Not Asserted
1	Copy Once
2	Copy No More
3	Copy Never - Zero Retention Not Asserted
4	Copy Never - Zero Retention Asserted
5 to 7	Reserved for future use

Table 8: Movement and Copying Propagation Information

movement_and_copying_propagation_information	Description
0	MLAD.
1	MGAD
2	MAD
3	MCPCM

Table 9: Viewing Propagation Information

viewing_propagation_information	Description
0	VLAD
1	VGAD
2	VAD
3	VCPCM

8.2 CPCM Auxiliary Data Syntax

The CPCM auxiliary data syntax is shown in Table 10. CPCM auxiliary data structure is securely bound to the CL but shall be transported independently as specified in TS 102 825-9 [3].

Table 10: CPCM Auxiliary Data structure

Syntax	Bits	Identifier
CPCM_auxiliary_data(){		
CPCM_auxiliary_data_element_counter	8	uimsbf
for (i=0; i<CPCM_auxiliary_data_element_counter; i++){		
CPCM_auxiliary_data_element_identifier	8	bslbf
[CPCM_auxiliary_data_element_length]	16	uimsbf
CPCM_auxiliary_data_element		
}		
}		

The encoding consists in a suite of CPCM auxiliary data elements identified by an identifier allocated as shown in Table 11. More details are given in TS 102 825-4 [2].

Table 11: CPCM auxiliary data element identifiers

Field Identifier	Field Name	Bits	Identifier	Description
0	original_full_USI	variable	bslbf	Original full USI as provided by the delivery system within the Acquisition Point. See TS 102 825-10 [4].
1	original_FTA_control	8	bslbf	Original signalling associated with a Free-To-Air content. See TS 102 825-10 [4].
2	geographic_location_information	variable	bslbf	Geographic location information for Content marked MGAD or VGAD. See TS 102 825-4 [2].
3	other_CPS_export_data	variable	bslbf	Proprietary data aimed at the other CPS to which the Content may be Exported. Other CPS can be Trusted, Controlled, or an Analogue Output. See TS 102 825-10 [4].
4 to 5	reserved			
6	CPCM_rights_issuer_URL	variable	bslbf	URL where additional Authorized Usage rights for the associated CPCM Content Item can be obtained.
7	CLC_private_data	variable	bslbf	Private data associated with the proprietary system from which the content was acquired.
8	CPCM_extension_data	variable	bslbf	Data destined for a CPCM extension.
9	private_extension_data	variable	bslbf	Data destined for a private extension.
10	key_recovery_information	variable	bslbf	Data destined for allowing recovery of the content scrambling key by an Authorized party.
11	external_scrambling_info	variable	bslbf	Data destined for an Acquisition Point to descramble and rescrumble content upon Acquisition.
12 to 255	reserved	variable	bslbf	Any newly defined element shall be accompanied by its corresponding CPCM_auxiliary_data_element_length field.

List of tables

Table 1: Key for USI to Manage Content within CPCM Device Groups	9
Table 2: Usage State Information Overview	12
Table 3: Simultaneous View Count Description	15
Table 4: Remote Access Rule Components	18
Table 5: Interpretation of remote_access_date	19
Table 6: CPCM USI	23
Table 7: Copy Control	24
Table 8: Movement and Copying Propagation Information	24
Table 9: Viewing Propagation Information	24
Table 10: CPCM Auxiliary Data structure	24
Table 11: CPCM auxiliary data element identifiers	25

List of figures

Figure 1: USI to Manage Content within CPCM Device Groups	9
---	---

History

Document history		
V1.1.1	July 2008	Publication
V1.2.1	March 2011	Publication