Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 1: CPCM Abbreviations, Definitions and Terms
## Contents

Intellectual Property Rights .................................................................................................................. 4
Foreword .................................................................................................................................................. 4
Introduction ........................................................................................................................................... 5

1 Scope .................................................................................................................................................. 6

2 References ........................................................................................................................................... 6
2.1 Normative references ....................................................................................................................... 6
2.2 Informative references ..................................................................................................................... 6

3 Definitions and abbreviations ............................................................................................................. 6
3.1 Definitions ....................................................................................................................................... 6
3.2 Abbreviations .................................................................................................................................. 10

4 Understanding the state charts .......................................................................................................... 11

5 CPCM Content flows ......................................................................................................................... 12

History ................................................................................................................................................... 13
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 ÉLECTrotechnique (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 1 of a multi-part deliverable covering the DVB Content Protection and Copy Management Specification as identified below:

TS 102 825-1: "CPCM Abbreviations, Definitions and Terms";
TS 102 825-2: "CPCM Reference Model";
TS 102 825-3: "CPCM Usage State Information";
TS 102 825-4: "CPCM System Specification";
TS 102 825-5: "CPCM Security Toolbox";
TR 102 825-6: "CPCM Security Test Vectors";
TS 102 825-7: "CPCM Authorized Domain Management";
TR 102 825-8: "CPCM Authorized Domain Management scenarios";
TS 102 825-9: "CPCM System Adaptation Layers";
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 Abbreviations, Definitions and Terms used for the Digital Video Broadcasting (DVB) Content Protection and Copy Management (CPCM) system.

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.

Not applicable.

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 following terms and definitions apply:

acquire: receive and ingest content from outside the CPCM System into the CPCM System

Acquisition Point (AP): abstract CPCM Functional Entity where content Acquisition takes place

acquisition: receipt and ingestion of content that was outside the CPCM System into the CPCM System

Authenticated Key Exchange (AKE): protocol establishing a Secure Authenticated Channel between two CPCM Instances

Authorized Domain (AD): distinguishable set of DVB CPCM compliant devices, which are owned, rented or otherwise controlled by members of a single household

NOTE: This definition makes no assumptions about the physical locations of the devices owned, rented or otherwise controlled by the members of the household

authorized domain management: managing function of the authorized domain
authorized domain size and extent: mechanism(s) to prevent an AD growing beyond a "reasonable" size

authorized usage: permitted usage of CPCM Content, consisting of the set of usage rules assertions applied to that content

blank device: device where the ADM functionality has not yet been initialized, or which has been reset to factory settings

NOTE: Such a device has no knowledge of any current authorized domain, not even a temporary local one.

consume: tangibly render content, or output Content constrained to inhibit any other usage

Consumption Point (CP): abstract CPCM Functional Entity where consumption is performed

consumption: tangible rendition of content, or a device output containing a transformation or signal that is intended to inhibit any usage other than the immediate conversion of the content to sound and vision

content item: discrete instance of Content of finite duration, e.g. a program/event or an incomplete segment thereof

content licence: securely maintained and communicated data structure containing the information necessary to manage the security of a CPCM content Item

content: data that is to be protected by the CPCM System

NOTE: 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.

controlled CPS: trusted CPS to which Export and Consumption Output can be enabled or disabled subject to USI

controlled export: digital output of CPCM Content mapped to a trusted CPS under the explicit control of the USI of that CPCM Content

copy (used as a noun): stored content item

copy (used as a verb): CPCM-managed process whereby a new stored content item is created from Acquired Content or from an existing stored Content Item

Copy Control Information (CCI): Usage State Information (USI) field that includes CCNA, C1, CNM and CN with and without zero retention

Copy Control Not Asserted (CCNA): Copy Control Information (CCI) state that means that the authorized usage will not include numerical restrictions to copying

Copy Never (CN): Copy Control Information state that means that the authorized usage will not permit copying

Copy No More (CNM): Copy Control Information state that means that the authorized usage will not permit copying

NOTE: This Copy Control Information state is given to copies of copy once content during the copying process.

Copy Once (C1): Copy Control Information state that means that the authorized usage will permit exactly one copy

NOTE: The resulting copy is marked "copy no more".

Countable Instance of CPCM Functionality (CICF): CPCM Instance that is capable of consumption or export and that has the appropriate bit set within its CPCM Instance Certificate to indicate that it shall be counted in the context of ADSE

CPCM Device: device that hosts one or more CPCM Instances

CPCM extension: extended, and either proprietary or standardized functionality that can have access to CPCM Content in accordance with a future CPCM compliance regime

CPCM instance: conformant implementation of any CPCM functionality

CPCM instance Certificate (CIC): unique certificate of a CPCM instance
CPCM scrambler: scrambling tool used to encrypt CPCM Content in the CPCM System

CPCM system: set of all compliant CPCM Devices

destination: destination of content that is being accessed from an Acquisition Point, Processing Entity or a Storage Entity

NOTE: E.g. another Storage Entity or Processing Entity, a Consumption Point or an Export Point.

device application: any non-CPCM functionality within a CPCM device

domain controller: global logical function providing overall control of the ADSE functions of an Authorized Domain, either residing in a single CPCM instance (though moveable), or distributed among a defined maximum number of CPCM instances

Export Point (EP): abstract CPCM functional entity where CPCM Content leaves the CPCM system

export: release of CPCM Content from explicit protection and management by the CPCM system to a Controlled CPS, a Trusted CPS or an Untrusted Space

functional entity: one of acquisition point, storage entity, processing entity, consumption point or export point

geographic area: defined geographic area that could be on the scale of a city, region, state, province, country or group of countries

Geographically-constrained AD (GAD): set of all CPCM Devices that are members of the same AD and that are also located in the same Geographic Area

Household: social unit consisting of all individuals who live together, as occupants of the same domicile.

input: device interface or CPS used to receive CPCM content or input content.

live/direct: live/direct viewing is defined as the consumption of content either:

i) "live" from the stream without entering the storage function for any purpose apart from that needed to support pause/trick play; or

ii) "directly" from a recording on an integrated storage entity under either the local, or remote, control of an external authority

Local Environment (LE): set of all Local CPCM devices

Local Master (LM): ADM function within a single local CPCM Instance that takes primary responsibility for responding to ADM requests for the AD of which it is a member

local: within the immediate vicinity, approximating to the physical extent of a domicile or vehicle

Localized AD (LAD): set of all Local CPCM instances within the AD

move: process of making a Copy wherein the original is then removed, erased or made no longer accessible

output: device interface or CPS used to transmit CPCM content, consumed content, or exported content

Processing Entity (PE): abstract CPCM Functional Entity where CPCM content is processed

processing: CPCM compliant operation upon encrypted or unencrypted content other than for consumption or export

EXAMPLE: Where CPCM content undergoes a permitted transformation from its original form to create new transformed CPCM content, or where information is extracted from the content such as audio volume levels or still images.

propagation: viewing, copying and movement within or beyond certain "propagation realms" comprising:

- the Local Environment (LE);
- the Localized AD (LAD);
• the Geographically-constrained AD (GAD);

• the Authorized Domain (AD) and the CPCM system.

**proximity test**: means to determine whether two CPCM Devices, or a CPCM Device and a non-CPCM device storing CPCM content, are Local with respect to each other at the time the test is performed

**random value**: newly generated value output from a random number generator compliant with applicable CPCM C&R regime

**remote access**: access to CPCM content from outside the local environment or localized AD from which that CPCM content is sourced

**retrieval**: access to a Copy of CPCM content

**Secure Authenticated Channel (SAC)**: virtual communications channel established between CPCM Instances for the transfer of certain CPCM data

**sink (used as a noun)**: sink of content, e.g. a processing entity, storage entity, consumption point or export point

**sink (used as a verb)**: act of receiving content by a sink

**source (used as a noun)**: source of content, e.g. an acquisition point, processing entity or storage entity

**source (used as a verb)**: act of emitting content from a source

**Storage Entity (SE)**: abstract CPCM functional entity where a CPCM content Item can be stored, if copying is allowed, and from which that resulting copy can be retrieved

**storage medium**: fixed or removable physical medium that together with a storage and retrieval system comprises a storage entity

**trusted CPS**: 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 particular CPCM compliance regime that bestows this trust

**trusted export**: digital output of CPCM content mapped to a trusted CPS

**trusted source**: system or entity which is able to provide input content for the CPCM system on the grounds of explicit approval of that system or entity and/or its compliance with the CPCM compliance specification

**untrusted export**: digital output of CPCM content to untrusted space

**untrusted space**: any system, entity, device, component, medium, function, interface or any other tangible or intangible thing other than the CPCM system and all trusted CPSs

**usage rule**: particular operation upon, or behaviour of content to be controlled within the scope of the CPCM system

**Usage State Information (USI)**: CPCM content metadata that signals the authorized Usage for each CPCM content item

**view**: See consume.

NOTE: This also includes listen for audio only content.

**viewing**: See consumption.

NOTE: This also includes listening for audio only content.
3.2 Abbreviations

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

AAA Authorized Authenticated Agent
AD Authorized Domain
ADID AD Identifier
ADID AD Identifier
ADM Authorized Domain Management
ADMAAA AD Membership Assignment by Authorized Authenticated Agent
ADS AD Secret
ADSE Authorized Domain Size and Extent (enforcement)
AKE Authenticated Key Exchange
AP Acquisition Point
APECS Acquisition, Processing, Export, Consumption, Storage
bslbf bit string, left bit first
C&R Compliance and Robustness
Cl Copy Once
CA Conditional Access
CAM Conditional Access Module
CBC Cipher Block Chaining
CCI Copy Control Information
CCNA Copy Control Not Asserted
CIC CPCM Instance Certificate
CICF Countable Instance of CPCM Functionality
CL Content Licence
CLID Content Licence Identifier
CN Copy Never
CNM Copy No More
CP Consumption Point
CPCM Content Protection and Copy Management
CPE Customer Premise Equipment
CPS Content Protection System
CRL Certificate Revocation List
CS Ciphertext Stealing
CW Control Word
DC Domain Controller
DMH The Domain Membership History ADSE tool
DNCS Do Not CPCM Scramble
DRM Digital Rights Management
DS Device Secret
DVB Digital Video Broadcasting
EP Export Point
FTA Free-To-Air
FTV Free-To-View
GA Geographic Area
GAD Geographically-constrained AD
GTTP GPS or Terrestrial Triangulation for Proximity
HMAC Hash Message Authentication Code
HN Home Network
IC Integrated Circuit
IP Internet Protocol
IPX Internetwork Packet Exchange
IV Initialization Vector
IVE Initialization Vector for Encryption
LAD Localized AD
LE Local Environment
LLL Lenstra Lenstra Lovacz algorithm
LM Local Master
LSA Local Scrambler Algorithm
LSB Least Significant Byte
4 Understanding the state charts

The notation used within CPCM State Charts is illustrated in figure 1.

Figure 1: Legend for State Charts
### 5 CPCM Content flows

Table 1 contain additional definitions surrounding the various types of CPCM Content flows.

**Table 1: CPCM Content flow definitions**

<table>
<thead>
<tr>
<th>Ref.</th>
<th>Content Flow Name</th>
<th>Definition</th>
<th>Composition/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>C.0</td>
<td>CPCM Content</td>
<td>Content protected and managed by the CPCM System</td>
<td>Acquired Content</td>
</tr>
<tr>
<td>C.0.E</td>
<td>Embedded-CL CPCM Content</td>
<td>CPCM Content with the associated Content Licence embedded within the Content Item and protected separately</td>
<td></td>
</tr>
<tr>
<td>C.0.O</td>
<td>Out-of-band CL CPCM Content</td>
<td>CPCM Content with the associated Content Licence maintained separately from the Content Item</td>
<td></td>
</tr>
<tr>
<td>C.0.S</td>
<td>Scrambled CPCM Content</td>
<td>CPCM Content that is protected by the application of the CPCM Scrambler</td>
<td></td>
</tr>
<tr>
<td>C.0.C</td>
<td>Clear CPCM Content</td>
<td>CPCM Content with the &quot;Do Not CPCM Scramble&quot; (DNCS) Usage Rule assertion applied.</td>
<td></td>
</tr>
<tr>
<td>C.0.1</td>
<td>Acquired Content</td>
<td>CPCM Content emanating from an Acquisition Point</td>
<td>N/A</td>
</tr>
<tr>
<td>C.0.2</td>
<td>Stored Content</td>
<td>CPCM Content held in a Storage Entity</td>
<td>N/A</td>
</tr>
<tr>
<td>C.0.3</td>
<td>Retrieved Content</td>
<td>CPCM Content emanating from a Storage Entity</td>
<td>N/A</td>
</tr>
<tr>
<td>C.0.4</td>
<td>Processed Content</td>
<td>CPCM Content emanating from a Processing Entity</td>
<td>N/A</td>
</tr>
<tr>
<td>C.1</td>
<td>Input Content</td>
<td>Content from a Trusted Source entering the CPCM System via an Acquisition Point</td>
<td>N/A</td>
</tr>
<tr>
<td>C.1.1</td>
<td>Protected Delivery</td>
<td>Input Content from a protected delivery regime (e.g. CA or DRM System)</td>
<td>N/A</td>
</tr>
<tr>
<td>C.1.2</td>
<td>Trusted Clear Delivery</td>
<td>Clear (unprotected) Input Content from a Trusted Source (e.g. broadcast tuner or broadband CPE).</td>
<td>N/A</td>
</tr>
<tr>
<td>C.1.3</td>
<td>Trusted CPS</td>
<td>Input Content from a Trusted CPS with a Usage Rules mapping to CPCM</td>
<td>N/A</td>
</tr>
<tr>
<td>C.2</td>
<td>Consumed Content</td>
<td>Content released from the CPCM System for Consumption only</td>
<td>Sound and Vision</td>
</tr>
<tr>
<td>C.2.1</td>
<td>Sound &amp; Vision</td>
<td>Tangible rendition of content</td>
<td>N/A</td>
</tr>
<tr>
<td>C.2.2</td>
<td>Consumption Output</td>
<td>Content output at a device interface containing a transformation or signal that is intended to inhibit any usage other than the immediate conversion of the output content to Sound &amp; Vision</td>
<td>Digital Consumption Output</td>
</tr>
<tr>
<td>C.2.2.1</td>
<td>Digital Consumption Output</td>
<td>Consumption Output at a digital interface</td>
<td>N/A</td>
</tr>
<tr>
<td>C.2.2.2</td>
<td>Analogue Consumption Output</td>
<td>Consumption Output at an analogue interface</td>
<td>N/A</td>
</tr>
<tr>
<td>C.3</td>
<td>Exported Content</td>
<td>Content released from the CPCM system and its realm of protection</td>
<td>Trusted Export</td>
</tr>
<tr>
<td>C.3.1</td>
<td>Trusted Export</td>
<td>Digital Content output from the CPCM system mapped to a Trusted CPS</td>
<td>N/A</td>
</tr>
<tr>
<td>C.3.2</td>
<td>Controlled Export</td>
<td>Digital Content output from the CPCM system mapped to a Trusted CPS, under the control of USI</td>
<td>N/A</td>
</tr>
<tr>
<td>C.3.3</td>
<td>Untrusted Export</td>
<td>Digital Content output from the CPCM system into Untrusted Space, at a digital interface or in a digital format</td>
<td>N/A</td>
</tr>
<tr>
<td>C.3.4</td>
<td>Analogue Export</td>
<td>Content output from the CPCM system at an analogue interface other than for Consumption</td>
<td>N/A</td>
</tr>
</tbody>
</table>
## History

<table>
<thead>
<tr>
<th>Document history</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.1.1</td>
</tr>
<tr>
<td>V1.2.1</td>
</tr>
</tbody>
</table>