ETSI TS 102 825-2 V1.1.1 (2008-07)

Technical Specification

Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 2: CPCM Reference Model

Reference
DTS/JTC-DVB-222-2

Keywords
broadcast, 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

Contents

Intellectual Property Rights 6
Foreword 6
1 Scope 7
2 References 7
2.1 Normative references 7
2.2 Informative references 7
3 Definitions and abbreviations 8
3.1 Definitions 8
3.2 Abbreviations 8
4 Introduction 8
5 CPCM System 9
6 CPCM Functional Entities and Content Types 13
7 CPCM Device 15
7.1 General 15
7.2 Logical Interfaces 16
7.2.1 User Interface 16
7.2.2 Device Interaction 17
7.2.3 CPCM Interaction 17
7.2.4 Non-Secure CPCM Communications 17
7.2.5 Secure Authenticated Channel 17
7.2.6 Proximity Control Communications 17
7.3 CPCM Instance 18
7.3.1 General 18
7.3.2 CPCM Instance Logical Interfaces 19
7.3.2.1 CPCM Control 19
7.3.2.2 ADM Control 19
7.3.3 Security Control 20
7.3.3.1 General 20
7.3.3.2 Secure Data Management 20
7.3.3.2.1 General 20
7.3.3.2.2 CPCM Instance Certificate and Private Key 21
7.3.3.2.3 Device Secret 21
7.3.3.2.4 AD Secret and AD Identifier 21
7.3.3.3 Trust Establishment 21
7.3.3.4 SAC Management 21
7.3.3.5 Licence Processing 21
7.3.3.6 Key Management 22
7.3.3.6.1 Content Key Management 22
7.3.3.6.2 Control Key Management 22
7.3.3.7 Cryptographic Tools 22
7.3.3.8 Proximity Control 22
7.3.3.9 Secure Time 23
7.3.3.10 Mapping to Other Content Protection Systems 23
7.3.4 Content Handling 24
7.3.4.1 General 24
7.3.4.2 CPCM A.P.E.C.S. 24
7.3.4.3 CPCM Scramble/Descramble 25
7.3.4.4 Embedded CL Handling 25
7.3.4.5 CPCM Content Decode 25
7.3.4.6 CPCM Content Digital-to-Analogue Conversion 25
7.3.4.7 Exchange to/from Other Content Protection Systems 26
7.3.5 Authorized Domain Management 26

7.3.5.1 General 26
7.3.5.2 AD Discovery 26
7.3.5.3 AD Membership Management 27
7.3.5.4 AD Name Management 27
7.4 Device Interfaces 27
7.5 Storage Drives and Media 29
7.6 CPCM Device and Non-CPCM Content 30

8 CPCM Authorized Domain 30
8.1 General 30
8.2 Authorized Domain Management 31

9 CPCM Usage Rules 32
9.1 General 32
9.2 Copy and Movement Control 33
9.3 Consumption Control 33
9.3.1 General 33
9.3.2 Tethered Content 33
9.3.3 Time-based Usage 33
9.3.4 Concurrent Usage 34
9.4 Content Propagation 34
9.4.1 General 34
9.4.2 Restrict to Authorized Domain 35
9.4.3 Restrict to Local Environment 35
9.4.4 Restrict to Localized Authorized Domain 36
9.4.5 Restrict to Geographically Constrained AD 37
9.4.6 Propagate to Untrusted Space 38
9.5 Output Control 38
9.6 Ancillary Control 39

10 CPCM Content 39
10.1 General 39
10.2 Content Licence 40
10.2.1 General 40
10.2.2 CPCM Version 40
10.2.3 Content Licence Identifier 40
10.2.4 Content Licence Creator 40
10.2.5 C&R Regime Information 40
10.2.6 Revocation Information 41
10.2.7 Authorized Domain Identifier 41
10.2.8 Content Descrambling Information 41
10.2.9 Usage State Information 41
10.2.10 Content License Management Data 41
10.3 CPCM Content Licence Maintenance 41
10.3.1 General 41
10.3.2 Out-of-band (Separate) Content Licence 41
10.3.3 In-band (Embedded) Content Licence 42
10.4 CPCM Content Licence Protection 42
10.4.1 General 42
10.4.2 CL Protection by SAC Session Key 42
10.4.3 CL Protection by Device Secret 43
10.4.4 CL Protection by AD Secret 43
10.5 CPCM Content Security 44
10.6 CPCM Clear Content 44
10.7 CPCM Content Item Delineation 44
10.8 CPCM Content Revocation 45
10.9 CPCM Content Recovery 45

11 CPCM Content Management 45
11.1 General 45
11.2 Basic Content Management Model 45
11.3 Acquisition 46
11.3.1 General 46

11.3.2 Protected Delivery 47
11.3.2.1 General 47
11.3.2.2 Conditional Access Integrated in the CPCM Device 48
11.3.2.3 Conditional Access Smart-Card 48
11.3.2.4 Conditional Access Module 50
11.3.2.5 Free-To-View Delivery 51
11.3.2.6 DRM System 52
11.3.3 Trusted Clear Delivery 54
11.3.4 Trusted Content Protection System 55
11.4 Storage 56
11.5 Processing 58
11.6 Consumption 59
11.6.1 General 59
11.6.2 Sound and Vision 60
11.6.3 Consumption Output 60
11.7 Export 61
11.7.1 General 61
11.7.2 Trusted Export 62
11.7.3 Controlled Export 62
11.7.4 Untrusted Export 62
11.7.5 Analogue Export 63
12 Extensions to CPCM 63
13 CPCM as an Interoperability Platform 64
History 67

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

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

The present document is part 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 [3].

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 Reference Model (Ref Mod) 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 a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

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

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

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 indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

Not applicable.

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

[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".

[i.3] ETSI TS 102 825-1: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM) Part 1: CPCM Abbreviations, Definitions and Terms".

[i.4] ETSI TS 102 825-4: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM) Part 4: CPCM System Specification".

[i.5] ETSI TS 102 825-3: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM) Part 3: CPCM Usage State Information".

[i.6] ETSI TS 102 825-5: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM) Part 5: CPCM Security Toolbox".

[i.7] ETSI TS 102 825-7: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM) Part 7: CPCM Authorized Domain Management".

[i.8] ETSI TR 102 825-8: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM) Part 8: CPCM Authorized Domain Management scenarios".

[i.9] ETSI TS 102 825-9: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM) Part 9: CPCM System Adaptation Layers".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 102 825-1 [i.3] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TS 102 825-1 [i.3] apply.

4 Introduction

The CPCM Reference Model provides a technical and architectural framework for the DVB Content Protection and Copy Management (CPCM) System.

The Reference Model is described on the basis of the CPCM Abbreviations, Definitions and Terms defined in TS 102 825-1 [i.3]. It provides a technology-agnostic basis for the CPCM System.

The CPCM System provides an interoperability platform for the protection and management of "commercial" content, i.e. not user-created content, in the consumer environment. The typical field of application of the CPCM System is shown in Figure 1.

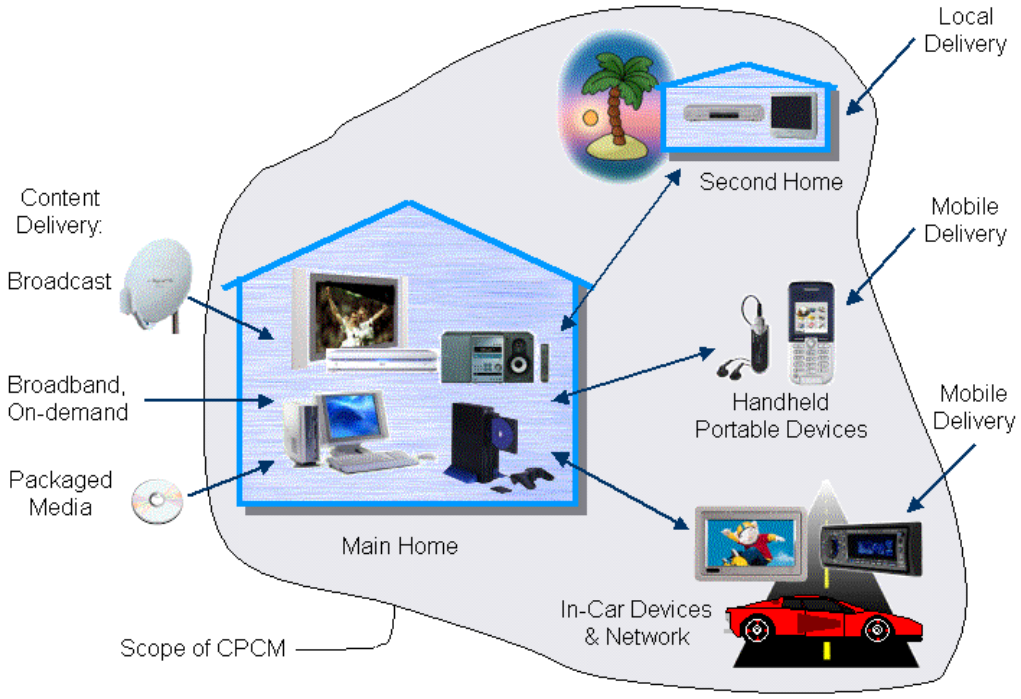

Figure 1: Scope of CPCM

The consumer environment contains many different kinds of devices that allow the user to enjoy content in different situations, for example stationary devices in the home, the same at any secondary residence, mobile devices in the car, or handheld portable devices. Content can be delivered to the consumer by various means, for example, via broadcast (cable, satellite or terrestrial), the Internet, from packaged media, or mobile delivery, as shown in Figure 1. CPCM intends to provide a protection and management environment that is relevant for all delivery channels, for all content usage scenarios and business models that are familiar to the user, and for those to come, on whatever types of device are deployed to let users access content.

It is impossible to document the CPCM Reference Model sufficiently in a single diagram, thus the CPCM Reference Model consists of several aspects, or views, which taken together deliver the full picture.

Clause 5 gives a high-level introduction to each of the various aspects that together define the CPCM System. Subsequent clauses then expand on each of these aspects to give the complete CPCM Reference Model.

5 CPCM System

This clause gives an overview of the various elements of the CPCM System.

Figure 2 shows the basic conceptual model of the CPCM System.

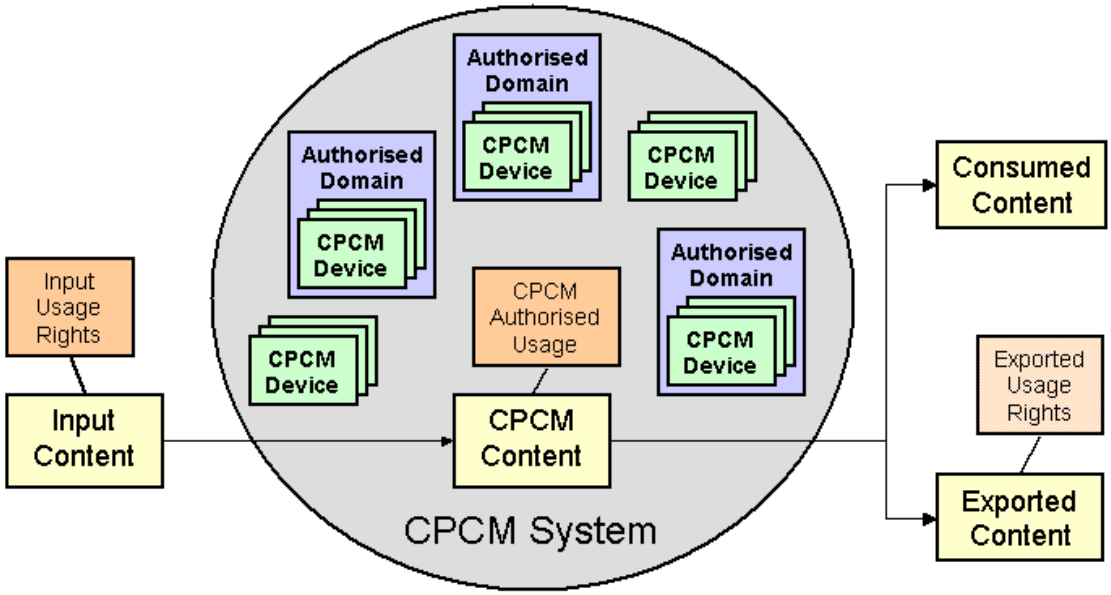

Figure 2: CPCM System Conceptual Diagram

It is intended that the CPCM System will be implemented for different methods of Input Content delivery to the consumer including free-to-air television, pay television and purchased media, on consumer equipment provided by many manufacturers, deploying various technologies to exchange and store content.

The basic CPCM content management model is that Input Content enters the CPCM System to become CPCM Content. CPCM Content is managed and protected within the CPCM System. CPCM Content leaves the CPCM System when it is Consumed by the user, or when Exported to another system.

CPCM Functional Entities.

The Reference Model defines the set of five abstract content management functions - Acquisition, Storage, Processing, Consumption, and Export - which cover all relevant content usage scenarios in the consumer environment. These functions map to the five CPCM Functional Entities - Acquisition Point, Storage Entity, Processing Entity, Consumption Point, and Export Point. Figure 3 shows the view of the CPCM System in terms of the set of abstract Functional Entities.

Thus Input Content that enters the CPCM System does so by being Acquired at an Acquisition Point, by a CPCM Device that implements that Acquisition Point, to become CPCM content. CPCM Content can be Stored or Processed by the corresponding Functional Entities (Storage Entity, Processing Entity), implemented on a CPCM Device. CPCM Content leaves the CPCM System when it is Consumed, at a Consumption Point, or Exported, at an Export Point. Again, these Functional Entities can be implemented inside any CPCM Device.

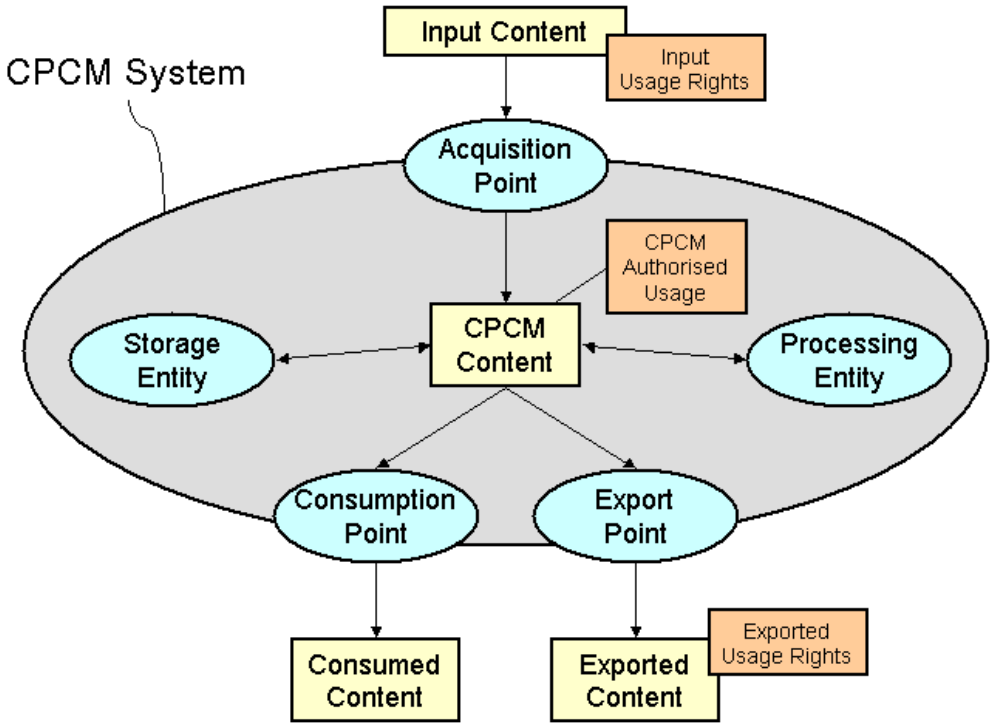

Figure 3: CPCM Functional Entities

The CPCM Functional Entities and basic CPCM Content types are described further in clause 6.

CPCM Device

A CPCM Device is any device that implements CPCM functionality in a compliant manner. As shown in Figure 2, the CPCM System can be considered as the complete set of all CPCM Devices.

The Reference Model makes no assumptions about the actual content handling functionality implemented within a CPCM Device. A CPCM Device can implement any combination of any of the abstract Functional Entities. Conversely, the content handling functionality of any relevant known device can always be mapped to a particular combination or sequence of any of the five CPCM abstract Functional Entities. The basic logical model of the CPCM Device and its generic content handling is shown in Figure 4.

The content handling implementations of the abstract Functional Entities are embedded in the CPCM Instance inside the CPCM Device. A CPCM Device can implement any other non-CPCM functionality, but this part of the device has no access to CPCM Content.

As well as the content handling functionality that implements whichever Functional Entities the CPCM Device includes, the CPCM Instance must include the CPCM Security Control functionality. This enables the CPCM Device to interoperate with other CPCM Devices to perform compliant exchange of CPCM Content and other CPCM functionality.

A CPCM Device can also implement any of the compliant methods to Acquire Input Content from Trusted Sources, Consume CPCM Content at the Device itself or via a compliant Consumption Output, or Export CPCM Content in a compliant manner. Each of these blocks of functionality is naturally secure in itself, but also the whole set of secure functionality, including the CPCM Instance, must be secure as a whole and would have to comply with the most stringent of compliance and/or robustness rules specified by the secure elements implemented in that CPCM Device.

CPCM Content that is exchanged directly between CPCM Instances in different CPCM Devices is inherently protected by the CPCM System.

A CPCM Device can also implement additional functionality in a CPCM Extension. CPCM Extensions are explained further towards the end of this clause.

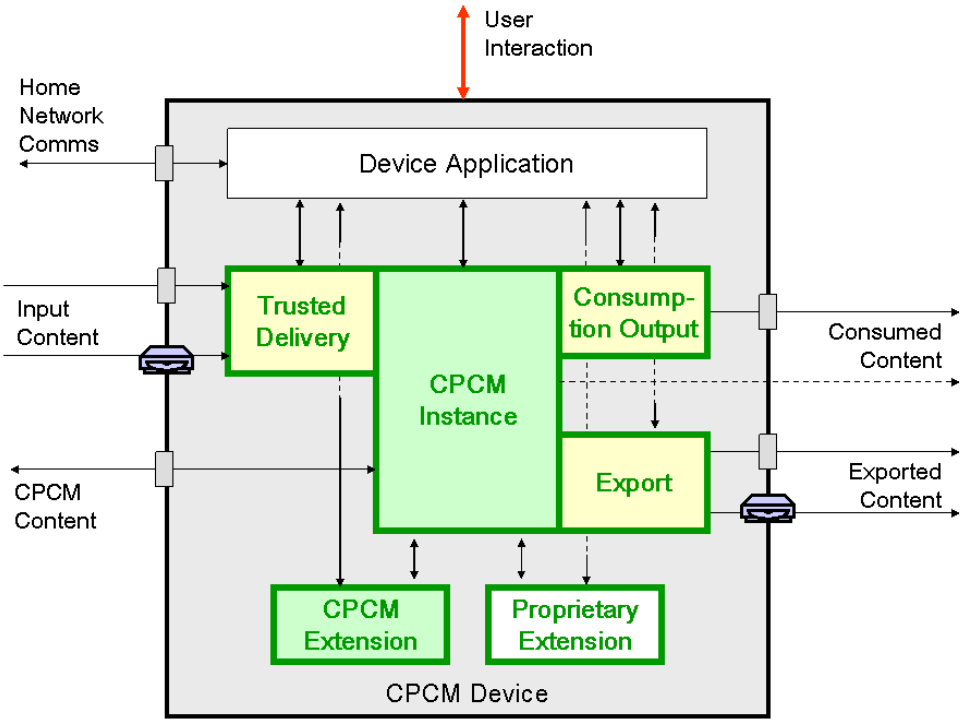

Figure 4: CPCM Device Basic Model

The CPCM Device and CPCM Instance are further elaborated in clause 7.

CPCM Authorized Domain

As shown in Figure 2, CPCM Devices can be logically grouped into Authorized Domains.

Looking back to Figure 1 shown in the Introduction, if all those devices belong to one household, then they would constitute that household's Authorized Domain (AD). Thus the Authorized Domain provides a destination for content that maps to the bounds of a single household.

In general terms the AD can be seen as the logical grouping of all the CPCM Devices belonging to one household, be those devices located in the main domicile, devices located at another domicile (e.g. holiday home), portable handheld devices that are only intermittently connected with the aforementioned stationary devices, or devices fitted in the vehicles(s) belonging to that household.

The AD is intended to be an autonomous logical group of devices, not requiring any external administration. However, there may be cases where the AD is linked to a particular service provider, who may offer to administer the AD as part of their service provision to the consumer.

Some CPCM Content provision models do not require the binding of content to an AD. As already indicated in Figure 2, it is not mandatory that a CPCM Device be AD aware. CPCM Devices that are not equipped with AD membership functionality either will not have access to content that is, or is to be, bound to an AD; or they may be able to perform their designed functions without contravening AD related Usage Rules, for example by handling such CPCM Content as if the AD consisted of only that single CPCM Device.

The CPCM Authorized Domain and its Management are elaborated in clause 8.

CPCM Content Usage Rules

The Authorized Usage for any item of CPCM Content is the set of usage assertions expressed in the CPCM Usage Rules tied to the content. The CPCM Usage Rules may be set by the content or service provider, or may be mapped from the form of delivery (e.g. free-to-air broadcast). The extent to which Storage, Consumption and Export operations might be able to be performed may be subject to the content's Authorized Usage.

CPCM defines a common set of Usage Rules that are available for any content provider to select from and accordingly derive the desired Authorized Usage for the content within the CPCM System. The set of CPCM Usage Rules is intended to be flexible enough to cover all applicable content protection and management models, but is also concise enough to maintain clear and relatively simple content usage models for the consumer.

The Authorized Usage of a Content Item is coded as CPCM Content metadata called Usage State Information (USI). CPCM Content is managed and protected according to the USI applied to each Content Item. Apart from the compliant USI state transitions that are carried out implicitly by the CPCM System, entities holding legitimate authorization over content within the CPCM System can perform other changes to a Content Item's USI state after Acquisition in the CPCM System.

The CPCM Usage Rules are detailed in clause 9.

CPCM Content

"Content" 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.

CPCM Content is Content that is protected and managed by, and in conformance with, the CPCM System.

A Content Item is a discrete instance of Content of finite duration. Each CPCM Content Item is accompanied by a Content Licence carrying the associated USI together with further CPCM metadata. The CPCM System can handle the Content Licence and the Content Item itself in different ways depending on the target functionality and/or usage rules enforcement required by the USI.

This aspect and CPCM Content in general is elaborated further in clause 10.

Clause 11 discusses the issues of CPCM Content management around each of the Functional Entities and their possible implementations.

CPCM Extensions

The aspects of CPCM described so far define the baseline CPCM System. The baseline provides CPCM functionality that is common to all content provision and usage models, and a basis for all foreseen business models. There may, however, be particular environments or content provision and usage models where Extensions to the CPCM baseline are needed.

Clause 12 deals explicitly with CPCM Extensions.

CPCM as an Interoperability Platform

Clause 13 charts out the aspects of the CPCM System that together could potentially enable its use as an interoperability platform for the protection and management of commercial content in the consumer environment.

6 CPCM Functional Entities and Content Types

The five content management operations (Acquisition, Storage, Processing, Consumption and Export) constitute the set of abstract CPCM Functional Entities.

This set of Functional Entities is sufficient to describe any foreseen audio-visual content handling process in the consumer environment. Figure 5 elaborates the Functional Entities and basic content types with their nominal shorthand notation in relation to the CPCM System, and shows the possible content flows into and out of the CPCM System and between the Functional Entities within the CPCM System.

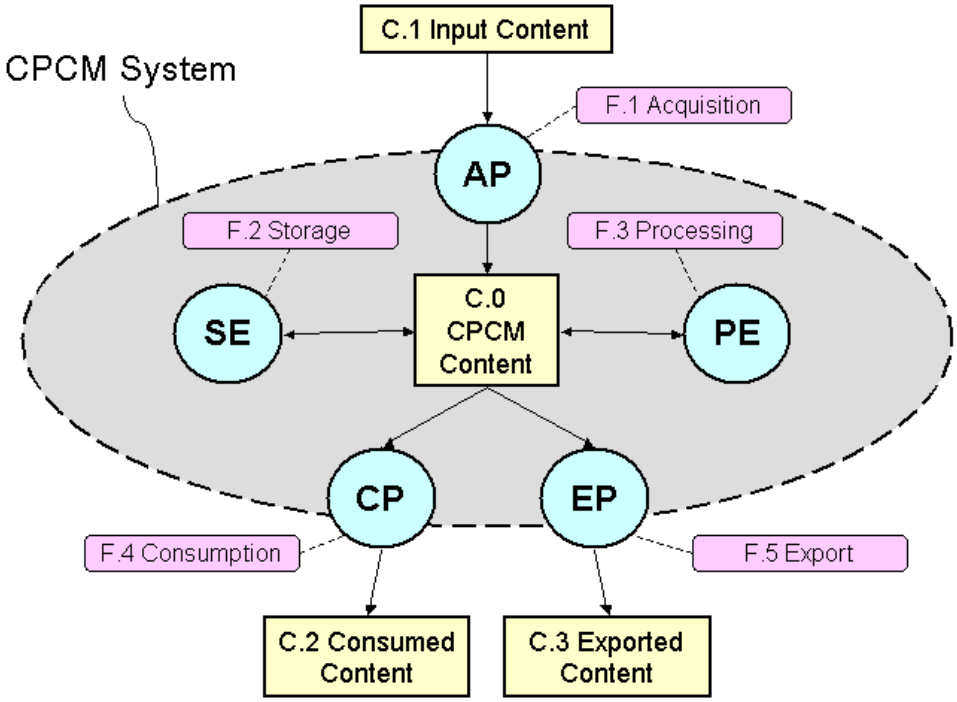

Figure 5: Abstract Model - CPCM Functional Entities and Content Types with Nominal Notation

Input Content is delivered from a Trusted Source and enters the CPCM System via an Acquisition Point (AP), performing the CPCM Function of Acquisition, to become CPCM Content.

The Storage Entity (SE) performs the CPCM Function of Storage, to store static instances, or Copies, of CPCM Content.

The Processing Entity (PE) performs the CPCM Function of Processing, which is any kind of allowed transformation (defined by C&R regime, for example) performed upon CPCM Content.

The Consumption Point performs the CPCM Function of Consumption. CPCM Content becomes transformed into a tangible content rendition, e.g. sound and light, at the Consumption Point, to become Consumed Content.

The Export Point performs the CPCM Function of Export. CPCM Content leaves the CPCM System via the Export Point, to become Exported Content. Exported Content is no longer explicitly protected and managed by the CPCM System.

Thus the abstract "Points" (Acquisition, Consumption and Export) are Functional Entities that have an abstract interface into or out of the CPCM System. The abstract "Entities" (Storage and Processing) are inside the CPCM System.

For the purposes of Content Management within the CPCM System, CPCM Content (given the shorthand notation "C.0") is sub-divided into four Content sub-Types. These are depicted in Figure 6, which also introduces the respective derivations of the "C.0" shorthand notation.

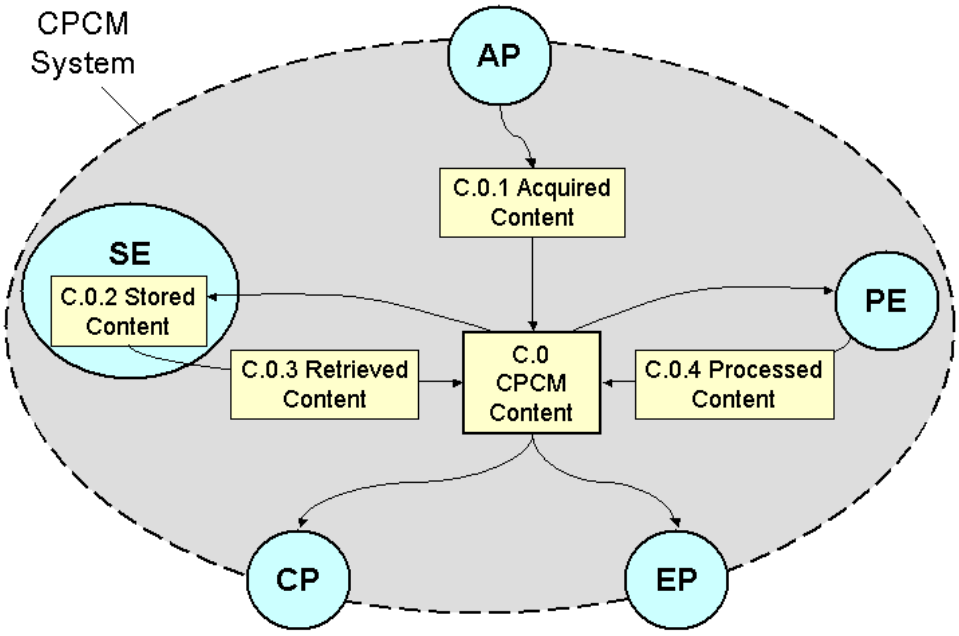

Figure 6: Abstract Model - Intra-CPCM Content types with Nominal Notation

Acquired Content (C.0.1) is CPCM Content emanating from the Acquisition Point, after Acquisition in the CPCM System.

Stored Content (C.0.2) is a static instance, or Copy, of CPCM Content held inside a Storage Entity.

Retrieved Content (C.0.3) is CPCM Content emanating or being pulled from a Storage Entity.

Processed Content (C.0.4) is CPCM Content emanating from a Processing Entity.

7 CPCM Device

7.1 General

A CPCM Device is a device that implements any CPCM functionality in a compliant manner. The implementation of CPCM functionality is referred to as a CPCM Instance. The CPCM functionality described so far in clause 6 covers only one part of what is required to implement CPCM, namely the Content Handling part. This clause describes the complete CPCM Instance in terms of a more specific functional model, including intra-CPCM functional interfaces, inter CPCM-Instance interfaces, and how the CPCM Instance relates to any non-CPCM functionality hosted by the CPCM Device.

Once the concepts of CPCM Device and CPCM Instance are established, this clause also deals with the more real-world aspects of how CPCM Devices exchange Content, using Device Interfaces and Storage Media.

Figure 7 shows the Logical Model of the CPCM Device, and the various logical interfaces and information flows involved. This diagram omits any non-CPCM secure Content handling for Acquisition, Consumption and Export.

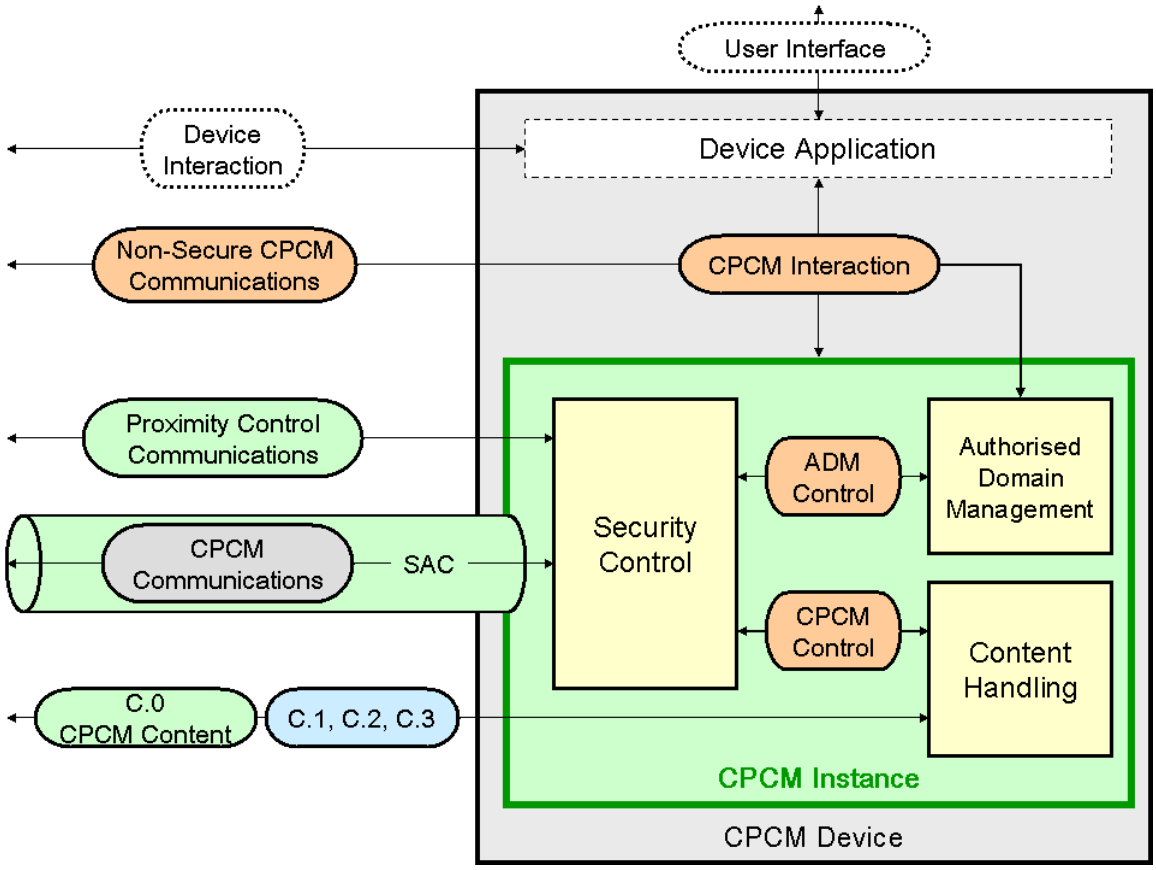

Figure 7: Logical Model - CPCM Device

A CPCM Device is a device that hosts one or more CPCM Instances.

A CPCM Device can also contain some other non-CPCM compliant function in addition to its CPCM functionality. CPCM Content handling is performed only by the CPCM Instance inside the device. The non-CPCM part of the device has no access to CPCM Content.

The CPCM Device can also host non-CPCM secure functionality, for the secure Acquisition of Content from other protection systems, or the secure Export (or possibly Consumption) of CPCM Content.

7.2 Logical Interfaces

7.2.1 User Interface

Naturally the CPCM Device's actual user interface and method of user interaction are outside the scope of the CPCM Reference Model. However, the following information must be able to be conveyed to the user:

- Information about the CPCM Authorized Usage of CPCM Content Items that the user that the user attempts to access, or are available to the user.
- Explanation of the CPCM Authorized Usage that prevents a user from performing an action.
- Information when access to CPCM Content is denied due to CPCM revocation of the Device's access to that content.

7.2.2 Device Interaction

The Device Interaction interface is realized through the connection between two or more devices. Typically this is a home networking protocol although it can be any bidirectional signalling mechanism.

Although this logical interface is outside the scope of CPCM, it does map very specifically to CPCM functions. If any CPCM Interaction takes place as a result of Device Interaction then this ideally happens completely transparently for the Device Interaction interface.

Device Interaction contains the following content services:

- Content discovery.
- Content selection.
- Content usage control and status (playback, trick-play, recording, etc.).

Device Interaction may carry information about the Content's Authorized Usage in a purely informative manner, but the definitive Authorized Usage associated with the CPCM Content will be contained in the Content Licence, described in clause 10.2.

7.2.3 CPCM Interaction

This interface is not standardized within the CPCM specifications. It may be implemented in a proprietary manner inside a CPCM Device, or it might be made accessible as a published interface by the supplier of an implementation of a particular CPCM Instance.

At least the following information exchanges are necessary:

- Obtain information about the Authorized Usage of any Content Item that can be accessed by the Device. This information is derived from the Content Licence, whenever applicable.
- Request access to a CPCM Content Item that is under the control of the present CPCM Instance.

7.2.4 Non-Secure CPCM Communications

This logical interface is used for all communications between CPCM Instances that need to be carried out over unsecured communication links, for example ADM or CPCM related discovery operations that occur prior to the establishment of a SAC.

Non-secure CPCM communications are transactions that do not require either security or trust that two communicating CPCM Instances are CPCM compliant.

7.2.5 Secure Authenticated Channel

The Secure Authenticated Channel (SAC) is a virtual communications channel established between mutually authenticated CPCM entities using a shared secret non-permanent key for secure and confidential transfer of data. In the CPCM Reference Model the SAC is established between the Security Control parts of CPCM Instances.

The various CPCM relevant data transferred via the SAC is collectively referred to as CPCM SAC Communications.

CPCM SAC Communications include ADM communications that do need to be secure. These are conveyed between ADM and Security Control via the ADM Control logical interface (see clause 7.3.2.2).

7.2.6 Proximity Control Communications

Proximity Control Communications are any communications necessary to securely establish whether or not two CPCM Instances are in the same Local Environment. These communications must of course provide a reliable, at least Boolean, indication of proximity, but they do not necessarily take place within the SAC. The method of Proximity Control might be network technology dependent and is defined in TS 102 825-4 [i.4].

7.3 CPCM Instance

7.3.1 General

The CPCM functionality inside a CPCM device is encapsulated in a logical entity called the CPCM Instance.

The CPCM Instance must be a compliant and secure implementation of its respective CPCM functionalities in accordance with one or more C&R regimes.

The implementation of the abstract Functional Entities within the CPCM Instance is outside the scope of the Reference Model. It is the CPCM Instance within a CPCM Device that must adhere to the requirements of the CPCM System, not the individual implemented Functional Entities. Thus it is the CPCM Instance that enables interoperability between different implementations of CPCM functionality, not the abstract Functional Entities embedded therein.

An exchange of CPCM Content (or other content that is outside the scope of the CPCM Reference Model) between CPCM Devices takes place as a result of a user action (via the Device's User Interface) and/or Device Interaction. Both of these elements are outside the scope of CPCM, but some form of interaction with the CPCM Instance is necessary in order to actuate a compliant content transfer between the devices. Thus the CPCM Interaction element is the interface between the CPCM Instance and the CPCM Device's host application.

The functionality inside the CPCM Instance is split into three parts - Security Control, Content Handling and Authorized Domain Management. Their constituent functions are described in clauses 7.3.3, 7.3.4 and 7.3.5 respectively.

The implementation in any CPCM Instance of the constituent components of the CPCM Instance functionality described here depends on the purpose of the Device hosting that CPCM Instance. Not all of the CPCM Instance functionality described here is mandatory for every CPCM Instance. For example, a CPCM Device might not include any Content Handling functionality if it provides only security or AD membership functions and has no access to CPCM Content; or some Devices might not need to be AD aware, so will thus omit the AD Management functionality.

A CPCM Instance that does not provide certain functionality might not need to include particular components. Conversely, a CPCM Instance that does not have certain tools will not be able to access Content that requires the component providing those tools.

Figure 8 shows the CPCM Instance with detail about the constituent functionality.

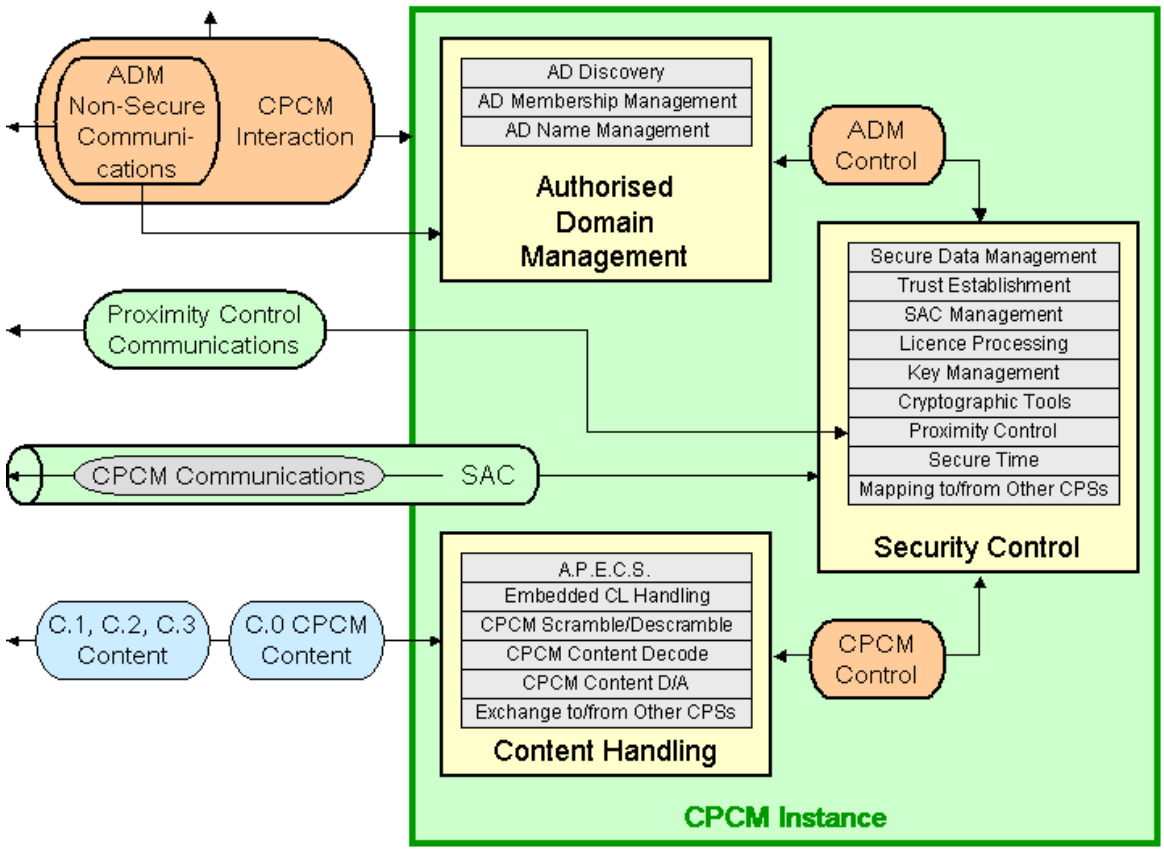

Figure 8: CPCM Instance Detail

7.3.2 CPCM Instance Logical Interfaces

7.3.2.1 CPCM Control

The CPCM Control interface provides the communication between the Security Control and Content Handling parts of the CPCM Instance.

The relevant information flows from the Security Control part to the Content Handling part are:

- Content scrambling or descrambling keys.
- Protected Content Licence to be embedded in a C.0.E CPCM Content Item (see clause 10.3.3).
- Control information.

The relevant information flows from the Content Handling part to the Security Control part are:

- Protected Content Licence extracted from a C.0.E CPCM Content Item (see clause 10.3.3).

7.3.2.2 ADM Control

The ADM Control logical interface contains the following functionality:

- Send and receive ADM relevant secure messages from another CPCM Instance.
- Retrieve the host Device's current AD Identifier (ADID), which is itself stored and managed within Security Control (see clause 7.3.3.2.4).
- Initiate an AD (Security Control creates AD Secret (ADS) and ADID pair (see clause 7.3.3.2.4), returns ADID to ADM).

- Join the AD (indicated by the ADID received from the other CPCM Instance that is admitting the present Device into the AD).

NOTE: The Security Control part will at the same time obtain ADS from that CPCM Instance on its own.

- Leave the AD (Security Control removes or deactivates current ADS/ADID pair as described in TS 102 825-7 [i.7]).

7.3.3 Security Control

7.3.3.1 General

Security Control provides all the security tools necessary to realize the CPCM functionality provided by the CPCM Instance.

Figure 9 shows the CPCM Instance with detail about the Security Control part.

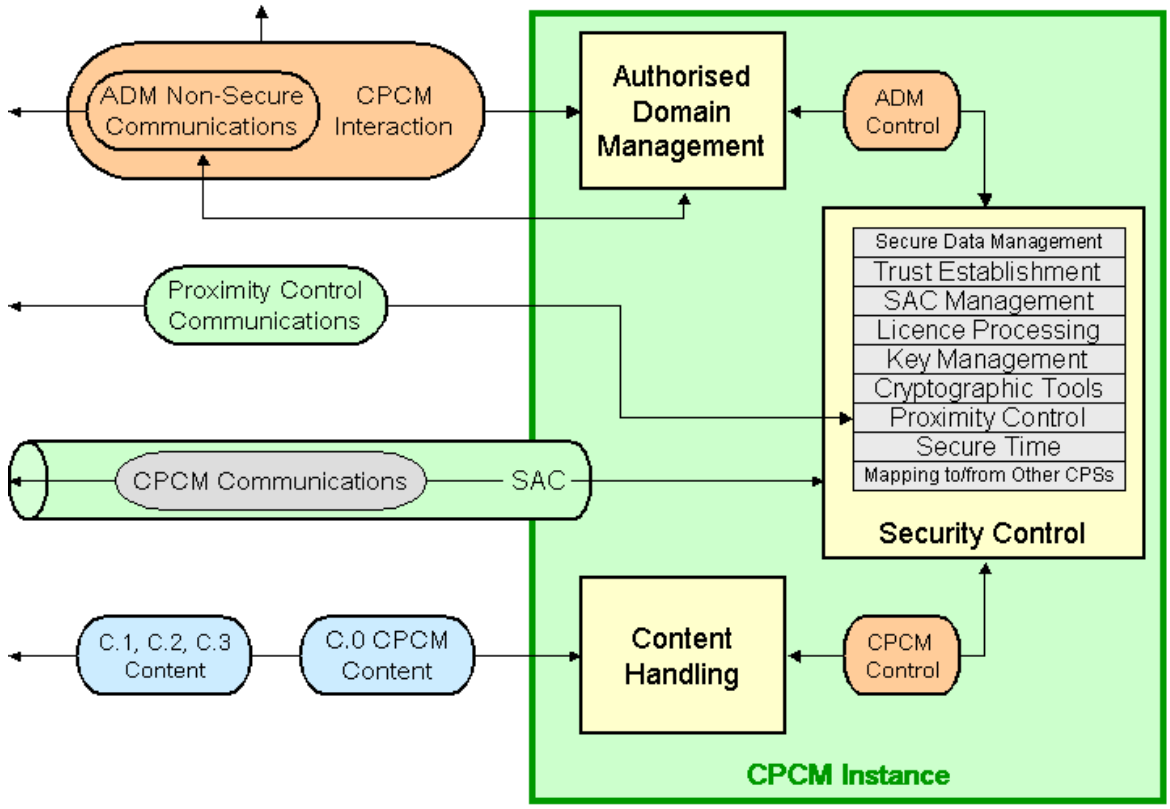

Figure 9: CPCM Instance with Detail on Security Control

The following clauses give a description of the functions of each of the components of Security Control.

7.3.3.2 Secure Data Management

7.3.3.2.1 General

This component is responsible for securely storing and maintaining all data that is applicable to CPCM security in the host device.

This component is responsible for securely storing and maintaining CPCM secret data in the host Device, such as any device secrets, private keys etc. associated with the CPCM Instance and/or the Authorized Domain to which it belongs.

CPCM Secure Data consists, potentially among others, of the CPCM Instance Certificate (CIC) and the AD Secret (ADS)/AD Identifier (ADID) pair of data fields.

7.3.3.2.2 CPCM Instance Certificate and Private Key

For the purposes of Trust Establishment with other CPCM Instances, each CPCM Instance (that needs to establish a SAC with other CPCM Instances) is equipped with a unique public key certificate, referred to as the CPCM Instance Certificate (CIC), issued by the, or a, Certificate Authority (CA).

The Secure Data Management element also securely maintains the corresponding private key uniquely associated with the CIC.

The format of the CIC is defined in TS 102 825-4 [i.4]. The certificate issuance regime is to be defined by each C&R regime.

7.3.3.2.3 Device Secret

The CPCM Instance might use a Device Secret (DS) in order to protect Content Licences created and/or maintained by that CPCM Instance. In that case the Secure Data Management element would maintain the DS.

7.3.3.2.4 AD Secret and AD Identifier

These data fields are required to be maintained only if the host device is AD aware. If the device is not AD aware then the DS (previous clause) may surrogate for the AD Secret for the purposes of handling CPCM Content that is to be bound to the AD (see clause 9.4.2).

The AD Secret (ADS) is a globally statistically unique secret of the AD. In certain cases it can be used to protect CPCM Content that is bound to that AD. This aspect is described in clause 10.

The AD Identifier (ADID) is a unique public identifier of the AD. It is derived from the ADS such that the ADS is not able to be derived on the basis of knowledge of the ADID. The ADID is used for AD discovery and membership management in ADM. This is described in clause 7.3.5.

The ADS and ADID pair of any AD remain constant throughout the life of that AD. The establishment of a new AD necessitates the creation of a new ADS/ADID pair. Changes in a CPCM Instance's ADS and ADID might occur as a result of a change in the host Device's AD membership, for example when leaving an AD, when the Device's ADS and ADID are deleted, or joining a different AD, when the Device's ADS and ADID adopt the values for that AD.

Secure Data Management may also need to store the ADS/ADID pairs of previous ADs of which the Device was previously a member. The exact requirements for such data are defined in TS 102 825-7 [i.7].

7.3.3.3 Trust Establishment

Trust is established between two CPCM Instances by the mutual exchange of CPCM Instance Certificates and their mutual verification. There may also be a revocation check performed on the received CIC on each side. This is described further in clause 10.8. Mutual exchange of CIC is done during SAC management (see clause 7.3.3.4).

Corresponding certification and revocation mechanisms are defined in TS 102 825-5 [i.6].

7.3.3.4 SAC Management

This component executes the task of SAC establishment with another CPCM Instance. The SAC is controlled by a volatile key that is derived through a process of a certificate-based authenticated key exchange. SAC control keys are managed by the Control Key Management component (see clause 7.3.3.6).

The SAC volatile key is computed by the two CPCM Instances during the Authenticated Key Exchange Protocol.

The actual SAC and AKE management protocols are defined in TS 102 825-5 [i.6].

7.3.3.5 Licence Processing

The core function of this component is to interpret the contents of the Content Licence in order to enforce compliant behaviour with respect to the associated CPCM Content Item within the host CPCM Device.

For each CPCM Content transaction, the Content Licence can arrive by two different paths:

a) The Content Licence arrives from the other CPCM Instance asynchronously via CPCM Secure Communications.

b) The Content Licence is embedded within the CPCM Content Item, in which case the Content Handling part of the CPCM Instance provides the protected Content Licence to the Licence Processing component of Security Control.

CPCM Licence Processing consists of:

- Decrypting the encrypted part of the licence (whenever applicable), by means of the Cryptographic Tools.
- Authenticating the license, by means of the Cryptographic Tools (whenever applicable).
- Interpreting the Content Licence against the CPCM Interaction request.
- Updating the Content Licence when required by the CPCM action (e.g. changing Copy Once to Copy No More or inserting content keys when content has to be locally scrambled).

7.3.3.6 Key Management

7.3.3.6.1 Content Key Management

This component has the following tasks:

- Generation of new Content Key/s as required by the Content Handling part of the CPCM Instance for local content scrambling (Acquisition, Processing).
- Provision of existing Content Keys, obtained from the respective Content Licences, as required by the Content Handling part of the CPCM Instance for local content descrambling (Consumption, Processing, Export), subject to the Authorized Usage for the respective CPCM Content, indicated by the USI in the Content Licence.

7.3.3.6.2 Control Key Management

This component is responsible for the management of control keys such as the SAC session keys and Authorized Domain keys, i.e. their creation, expiration or other operations upon them.

7.3.3.7 Cryptographic Tools

The Security Control element of a CPCM Instance must include the set of CPCM cryptographic tools necessary to implement the CPCM functionality hosted in that CPCM Instance, in accordance with CPCM System specification and C&R regimes.

The CPCM Security Toolbox (TS 102 825-5 [i.6]) includes:

- Cipher with the appropriate mode of operation for the SAC.
- Data integrity verification.
- Local Scrambling Algorithm.

How these tools are used is defined in other normative parts.

7.3.3.8 Proximity Control

This component performs the Proximity Test, as and when required by the Authorized Usage of the Content Item being transferred. The Proximity Test is the 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. The test may also be run in advance of content exchange, or on a periodic or irregular basis, and the result maintained for a reasonable period of time thereafter.

The Proximity Test shall be secure and authenticated, and the protocol robust. It may be a test that is specific to the communication link at hand, or independent of the network technology, for example it may work at the communication protocol layer. It may also comprise multiple tools. Proximity Test tools could work within the CPCM System, i.e. involve secure CPCM Communications between the two CPCM Instances performing the test, or they could rely on facilities outside of the CPCM System, i.e. Proximity Control in one CPCM Instance exercises such network facilities to determine Localness independently of the CPCM Instance (if present) in the other device.

The Proximity Test may also be used by Authorized Domain Management when determining whether a new device can join an AD.

Clause 9.4 describes how the Authorized Usage of the Content Item results in activation of this tool.

7.3.3.9 Secure Time

Secure Time control is needed for SAC management, in particular for SAC session timeout and renewal.

Secure Time management is also needed in CPCM Devices that are able to handle CPCM Content with time-based Usage Rules asserted (see clause 9.3.3).

The actual requirements of the Secure Time component, e.g. whether reliable absolute and/or relative time measurement is required, are defined in TS 102 825-5 [i.6].

Device implementations may maintain secure time in a variety of ways, for by example extracting reliable time signals from the broadcast, from a trusted Internet source, or from a known reliable internal clock.

CPCM may also define methods to communicate secure time among CPCM Instances, for example as part of CPCM Communications in the SAC or from a CPCM Extension.

7.3.3.10 Mapping to Other Content Protection Systems

If CPCM Content is Exported to, or Acquired from a trusted Content Protection System (CPS) (as requested by CPCM Interaction, and as possibly authorized by the Content Licence itself) a mapping has to take place, according to each C&R regime.

While the security mechanisms of the other CPS are outside the scope of CPCM, and are outside of the CPCM Instance in the Reference Model, such content transfers to or from other systems must be secure and robust, and may require encrypting and signing of the (mapped) Content Licence.

7.3.4 Content Handling

7.3.4.1 General

Content Handling includes the logical embodiment of any of the abstract Functional Entities described in the Abstract Model that are necessary to fulfil the device's intended functionality. Figure 10 shows the CPCM Instance with detail about the Content Handling part.

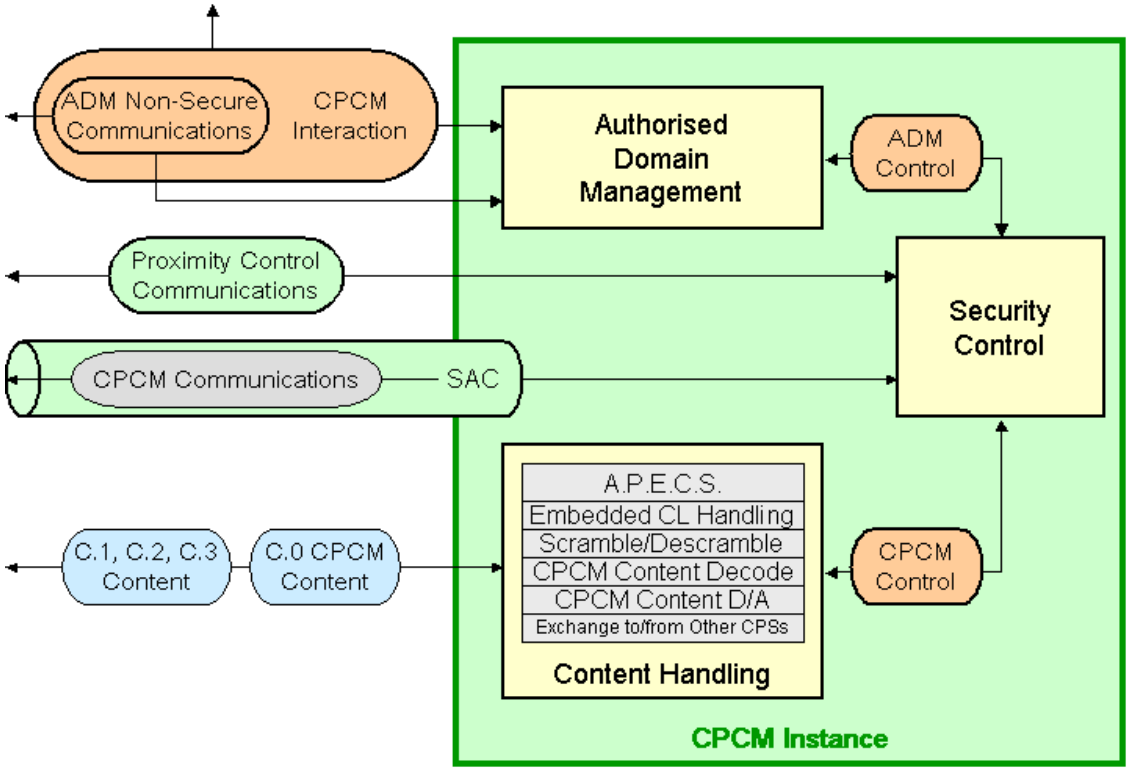

Figure 10: CPCM Instance with Detail on Content Handling

7.3.4.2 CPCM A.P.E.C.S.

CPCM A.P.E.C.S. refers to the complete set of content management functionality that can be implemented in a CPCM Instance, in terms of the CPCM abstract Functional Entities (Acquisition, Processing, Export, Consumption and Storage).

Figure 11 shows how the embodiments of the abstract Functional Entities of the Abstract Model are mapped to the Content Handling component of a CPCM Instance within a CPCM Device.

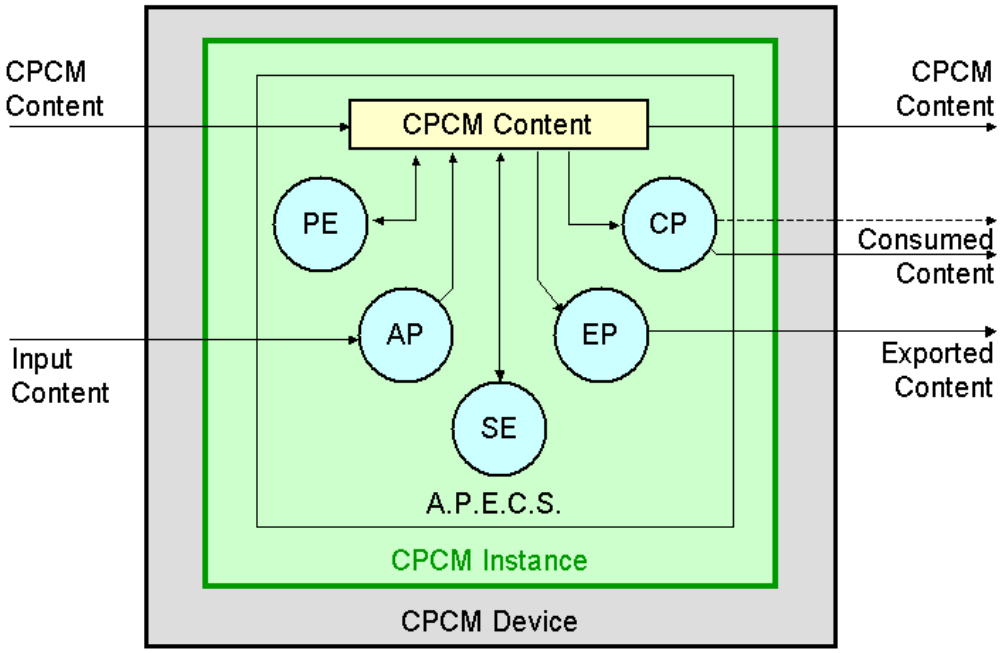

Figure 11: Logical Model - CPCM Instance and A.P.E.C.S.

This diagram shows how the different types of content are handled by a CPCM Device that nominally implements one of each of the abstract Functional Entities.

7.3.4.3 CPCM Scramble/Descramble

The Content Handling part shall include the CPCM scrambling tools if the Device functionality necessitates either scrambling and/or descrambling of CPCM Content handled by the CPCM Instance within that Device.

The inclusion of the CPCM Scrambler and CPCM Descrambler in a CPCM Device implementation is dictated by the nature of the Device and the Content Handling functionality of the CPCM Instance.

CPCM Devices that can Acquire or Process CPCM Content that needs to be scrambled in order to satisfy its Authorized Usage need to include the CPCM Scrambler, and Devices that can Process, Consume, or Export such CPCM Content need to include the CPCM Descrambler. CPCM Devices that provide only Storage functionality do not require the CPCM Scrambler or Descrambler.

7.3.4.4 Embedded CL Handling

This function performs the extraction and/or insertion of the CL into CPCM Content as appropriate for the case of C.0.E CPCM Content, described in clause 10.3.3.

The CL is passed to/from Security Control via the CPCM Control interface.

7.3.4.5 CPCM Content Decode

This function is the logical part of the content decoder(s) inside a CPCM Device that can decode CPCM Content.

7.3.4.6 CPCM Content Digital-to-Analogue Conversion

This function is the logical part of the digital-to-analogue (D/A) converter(s) inside a CPCM Device that can perform D/A conversion of CPCM Content.

7.3.4.7 Exchange to/from Other Content Protection Systems

This function performs any operation on CPCM Content necessary for its handover to the other CPS (for Export or to a Consumption Output), or any operation on the content coming in from another CPS (Acquisition) to become CPCM Content. The control of the content exchange is retained by the Mapping function in the Security Control part (see clause 7.3.3.10).

7.3.5 Authorized Domain Management

7.3.5.1 General

The Authorized Domain Management (ADM) function implements the AD Management rules for the CPCM Device. The basic ADM rules are described in clause 8. The inter-CPCM Instance protocols and exact mode of operation of ADM are defined in TS 102 825-7 [i.7].

ADM is an optional part of the CPCM Instance, as it is not always necessary that a CPCM Instance or Device be AD aware. A CPCM Device not being AD aware does not necessarily preclude its access to CPCM Content that is bound to an AD, or to Input Content that is signalled as requiring binding to an AD. This is dealt with further in clause 11.

If ADM is implemented in the CPCM Instance, then there is some functionality in Security Control which also needs to be implemented. This covers all secure data management and exchange needed for the purposes of ADM, and is described in clause 7.3.3.

ADM also requires some non-secure communications for the purpose of the AD-related discovery process. These communications can be either broadcast or point-to-point in nature.

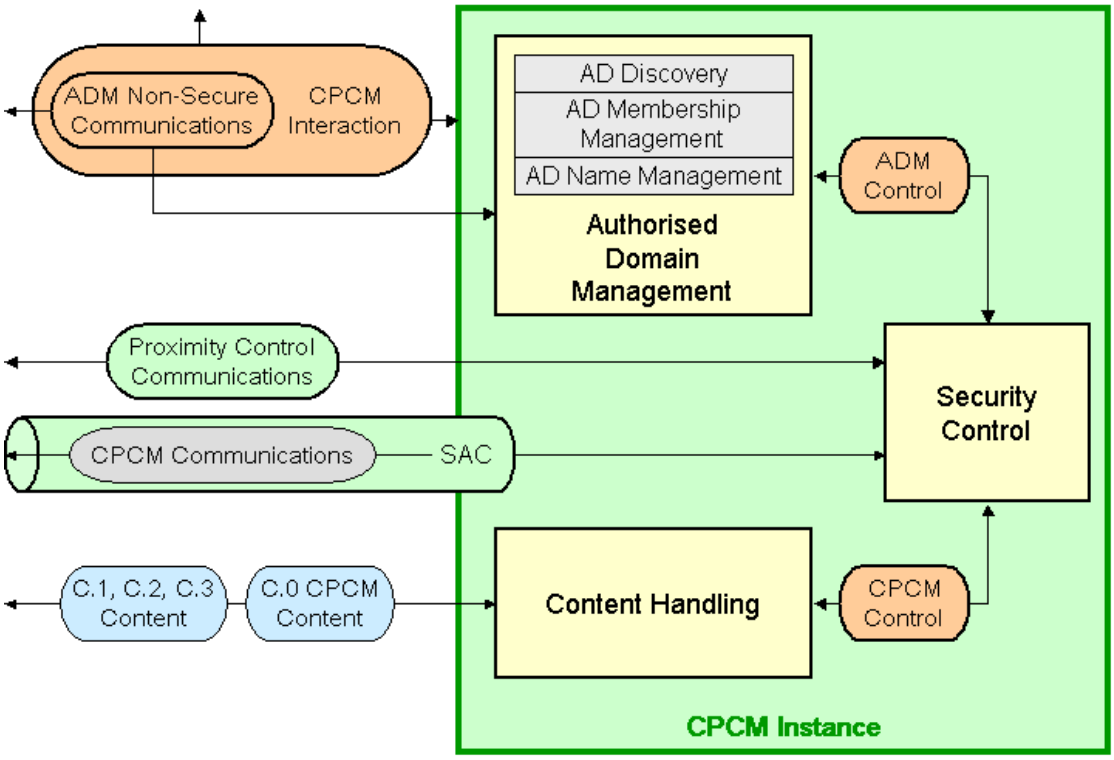

Figure 12 CPCM Instance with Detail on Authorized Domain Management

7.3.5.2 AD Discovery

AD Discovery provides signalling and procedures to determine the presence of any ADs when the CPCM Device hosting the present CPCM Instance is connected to other CPCM Devices in the network, and to advertise the AD membership of the present CPCM Instance to the other ADs, or the Device's "home" AD.

7.3.5.3 AD Membership Management

AD Membership Management manages the association of the present CPCM Instance with any AD. This covers the following cases:

- The process of joining any established and available AD.
- The process of leaving the AD of which the CPCM Instance is a member.
- The establishment of a new AD.

The AD Membership of a CPCM Instance is governed by the AD Identifier (ADID) that is stored in the Secure Data Management part of Security Control as the current AD for the CPCM Instance. The ADID is used for AD Discovery in Non-Secure ADM Communications. The ADID is described in detail in clause 7.3.3.2.

The AD Membership Management function interacts with Security Control in order to send and receive secure messages to/from the AD Membership Management function in other CPCM Instances, via the inter-CPCM Instance SAC, which is managed by the respective Security Control components.

ADM receives the current ADID from Secure Data Management in Security Control.

7.3.5.4 AD Name Management

The AD Name is a human-readable text to describe any AD. It is intended as an aid to users, and not as a tool to reliably identify any AD or perform the binding of content to the AD. Thus this is a feature that does not require any secure handling, but it does necessitate communications between CPCM Instances that are members of the AD.

This function handles the signalling and procedures for the assignment and modification of the human-readable name of the present AD.

The actual user interaction regarding the text of the name is handled by the Device Application and User Interface elements.

7.4 Device Interfaces

Consideration of Content flows into and out of CPCM Instances and Devices have hitherto been at an abstract level. Real CPCM Devices will exchange CPCM Content, Acquire Input Content, Export Content, and sometimes Consume Content via physical Device Interfaces.

Figure 13 shows the mapping of Device Interfaces to the Logical Model presented thus far. Treatment of the secure CPCM Communications is omitted in this diagram.

CPCM Content (C.0) can enter a CPCM Instance within a CPCM Device via a CPCM compliant Input interface, and can leave the CPCM Instance via a CPCM Output interface.

Input Content (C.1) can enter via an Input interface, and the Consumption Output (C.2.2) and Exported Content (C.3) can be transported via Output interfaces.

The terms Input and Output cover both cases: where only a physical Device interface is concerned; and the case where another Content Protection System (CPS) is associated with that interface.

Figure 13 shows this logical model with Inputs depicted on the left-hand side of the CPCM Device, and Outputs on the right-hand side.

This is still a logical representation, in that one physical device interface could realize more than one of these logical interfaces, both as Input and/or as an Output. In the Logical Model these interfaces are considered separately, while in the physical world the differentiation is on the Content that is transported via the respective physical interface.

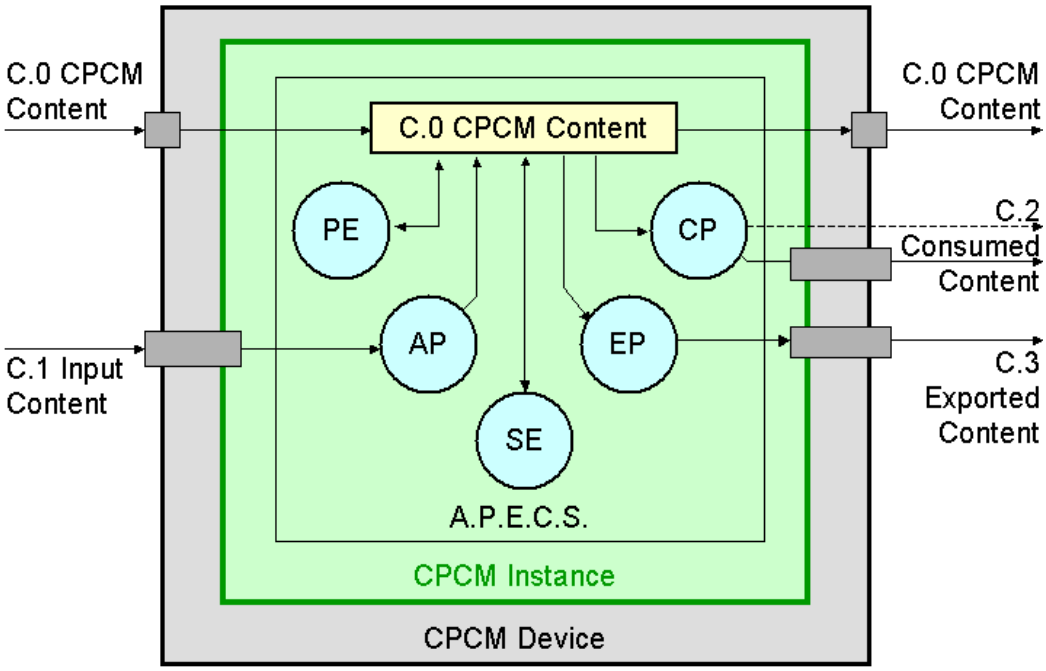

Figure 13: CPCM Device Interfaces

From Figure 13 it can be seen that the CPCM Device Interfaces straddle only the Device boundary. This is because the Content that they transport (CPCM Content) is protected by the CPCM System. Input Content, Consumption Outputs and Trusted and Controlled Exports need to be secured explicitly between the CPCM Device boundary and the CPCM Instance, the secure implementation of CPCM functionality.

No differentiation is made between digital and analogue Output interfaces at this stage. These are dealt with explicitly in clause 11.6 and clause 11.7.

To be considered as a possible tool, or more specifically a network interface (Input and/or Output) available for utilization by the CPCM System, that device network interface must be able to support the following:

- the establishment of a SAC across that interface; and
- the transport of CPCM Content.

Input interfaces, Consumption Outputs and Export interfaces are governed by the respective Trusted Source, Trusted CPS or Controlled CPS, and their agreed usage to be detailed by each C&R regime.

7.5 Storage Drives and Media

Content can also enter and leave CPCM Instances and Devices by way of storage media. Figure 14 shows, based on the examples of an internal hard-disk drive (HDD) and a removable media reader/writer drive, how physical storage provided in a CPCM Device maps to the CPCM Instance within that Device.

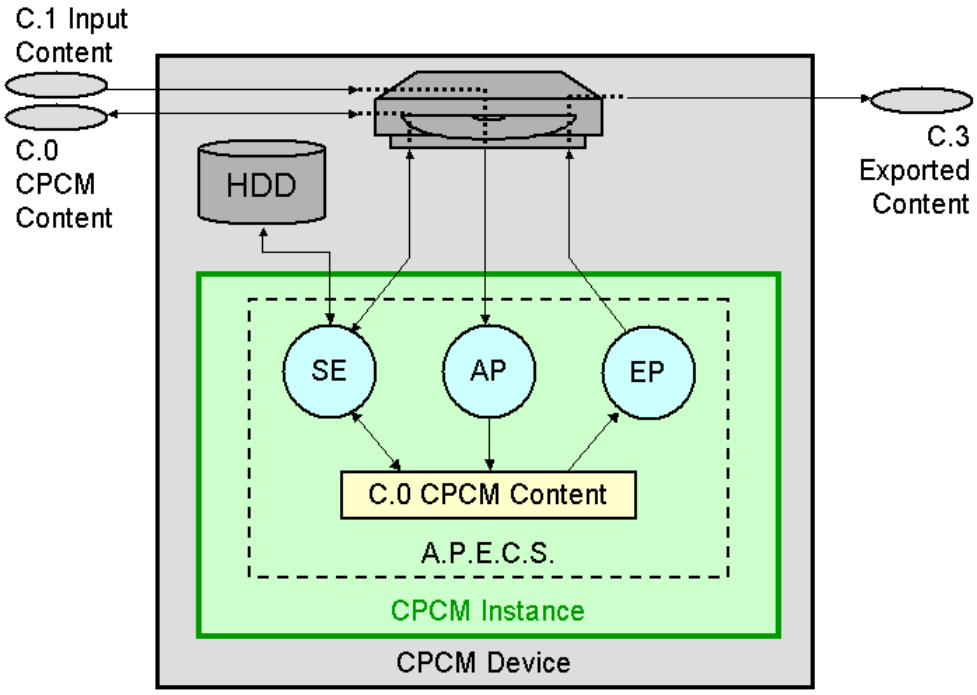

Figure 14: CPCM Device and Physical Storage

Content can be Acquired from, or Exported to established storage formats. Which formats are allowed in each case is outside the scope of the Reference Model. Such Acquisition and Export could, of course, also take place to/from embedded storage, for example a hard-disk drive, but this is not shown in Figure 14 for the sake of simplicity.

The CPCM Reference Model makes no distinction between fixed and removable storage, as there is no clear distinction in reality. Physical storage drives are always outside of the CPCM Instance. For the storage of CPCM Content in internal storage drives, no requirements on the security of the physical storage drive or medium are inferred by the CPCM System, because that content is always protected by CPCM, and it is the Content Licence function (inside the Security Control part of the CPCM Instance) that keeps the CPCM Content secure. In the logical model, it is the Storage Entity within the Content Handling part of the CPCM Instance that Stores the Content to, and Retrieves the Content from the drive or medium.

While the Reference Model makes no distinction in principle, there are practical implications for the Storage of CPCM Content on removable media when CPCM Content is intended to be truly portable on such media. Clauses 10 and 11 include further consideration of physical storage in dealing with the various Content management methods.

As with Device interfaces (clause 7.4), physical storage formats or media can carry CPCM Content (C.0), provide Input Content (C.1), or enable the Export of CPCM Content (C.3). There could also be an external CPS associated with the storage format. As explained further in clauses 11.4 and 11.7 respectively, which storage formats and/or external CPSs are deployed in each case is the subject for each C&R regime.

7.6 CPCM Device and Non-CPCM Content

A CPCM Device can also include non-CPCM functionality that handles non-CPCM Content. The non-CPCM functionality shall not have access to CPCM Content, and there shall be no mechanism for ingesting non-CPCM Content into the CPCM System other than the compliant Acquisition methods described in clause 11.3.

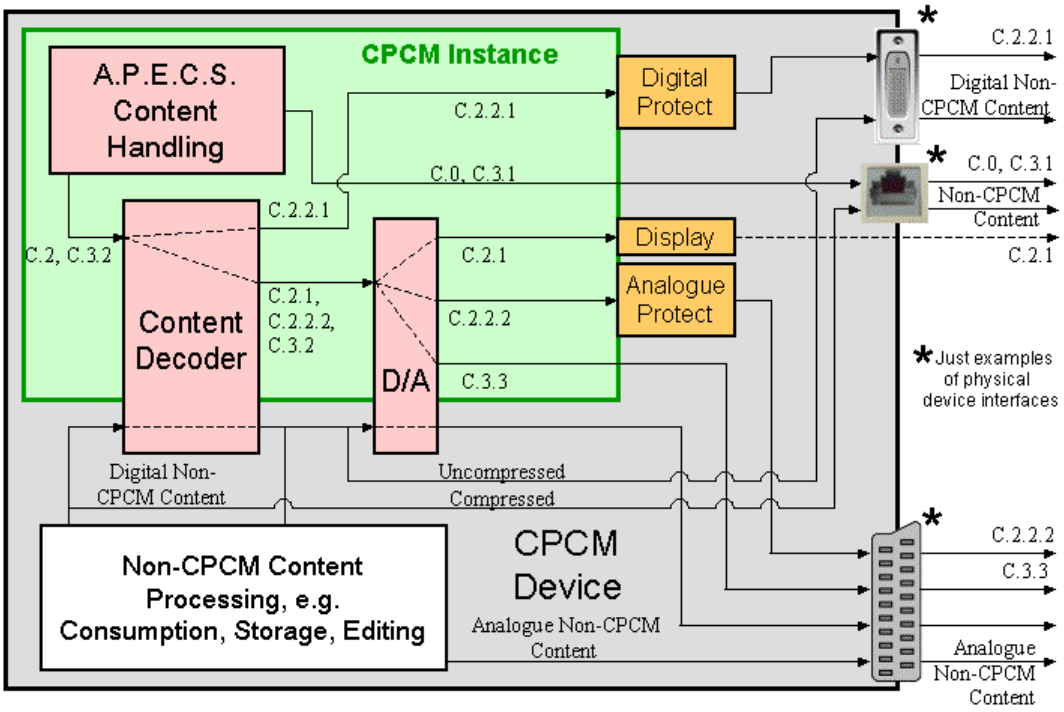

Figure 15: CPCM Device Outputs and Non-CPCM Content

The sub-categorizations of C.2 Consumed Content and C.3 Exported Content are explained in clauses 11.6 and 11.7 respectively.

As shown in the above diagram, some resources of a CPCM Device might be shared between the CPCM Instance and the non-CPCM functionality also hosted by that device. The CPCM Content paths must adhere to any CPCM compliance and robustness requirements set forth by its C&R regime.

Content entering at Device Inputs of a CPCM Device could be either CPCM Input Content (C.1) or non-CPCM content.

Content entering a Device Input that is not recognizable as CPCM Input Content will be treated as non-CPCM Content. It will never be Acquired by the CPCM Instance to become CPCM Content.

8 CPCM Authorized Domain

8.1 General

The Authorized Domain (AD) is a distinguishable set of DVB CPCM compliant devices, which are owned, rented or otherwise controlled by members of a single household. A household is considered to be the social unit consisting of all individuals who live together, as occupants of the same domicile. This makes no assumptions about the physical locations of the devices owned, rented or otherwise controlled by the members of the household.

In more general terms the AD can be seen as the logical grouping of all the CPCM Devices belonging to one household, be those devices located in the main domicile, devices located at another residence (e.g. holiday home), portable handheld devices that are only intermittently connected with the aforementioned stationary devices, or devices fitted in the car(s) belonging to that household.

It is not mandatory for all CPCM Devices to be AD aware. Thus, any household might own a mixture of CPCM Devices that belong to that household's AD, or that are not AD aware, but that nevertheless can interoperate with the AD aware Devices in accordance with the requirements of the CPCM System.

Looking back to Figure 1 shown in the Introduction, if all those devices belong to one household, then they would constitute that household's AD. This is shown in Figure 16.

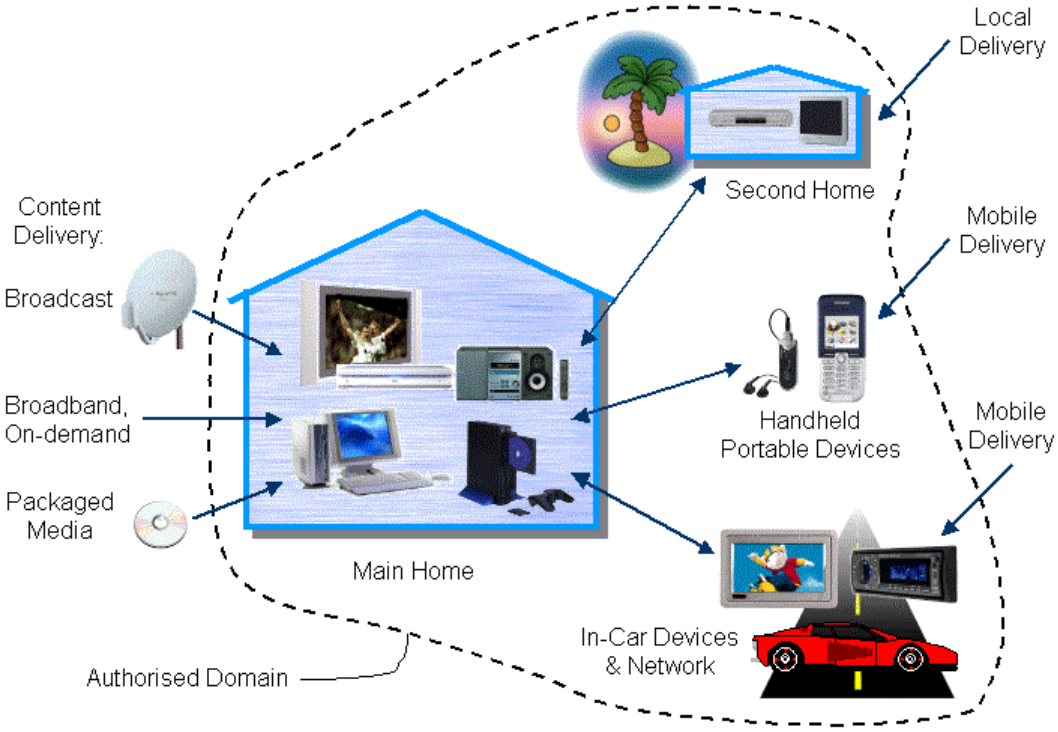

Figure 16: A Typical Authorized Domain

8.2 Authorized Domain Management

The following gives an outline of the general Authorized Domain Management aspects of the CPCM System. CPCM Authorized Domain Management (ADM) is the set of rules applying to the dynamic AD membership properties of CPCM Devices. The definitive ADM functionality, including how these requirements are addressed, is contained in TS 102 825-7 [i.7].

The Authorized Domain can be formed and managed autonomously. There is no requirement to be able to link a particular AD to its owner(s) or its location(s), although these modes of operation are not precluded.

An Authorized Domain has identifiable, discrete bounds that allow it to be distinguished from another AD. This is achieved by the controlled management of the AD membership of each of the user's devices, and by the possibility to bind CPCM Content to only one AD, if such binding is required by the content provider.

The AD is very much a physical entity, for which the expected mode of operation is that the user's devices somehow become members of his AD and thus gain access to content bound to the AD, in other words, content whose usage is restricted to the bounds of the user's AD, or his set of devices.

The process of creating an Authorized Domain requires minimal user interaction. Initially a single device is able to establish a new Authorized Domain. This process does not require connection with a back-office or any other 3rd party registration office.

The process of a device joining an Authorized Domain requires minimal user interaction. This process does not require connection with a back-office or any other third-party registration office. After joining an Authorized Domain, new devices will have access to content already existing in that Authorized Domain, as permitted by the USI.

The minimum size of an Authorized Domain is one device.

The DVB CPCM System has a means to limit the size and/or scope and/or extent of an Authorized Domain. This limitation should be effectively transparent and unnoticed by the overwhelming majority of all consumers. In addition, a fixed absolute maximum number of member devices might be set for any one AD. This means are defined in TS 102 825-7 [i.7].

A device's membership in an Authorized Domain is capable of being terminated. After termination of a device's membership in one AD the device may establish a new membership in another AD.

All devices in an aggregated AD will have access to AD-bound CPCM Content brought in from contributing ADs. The content's original USI is preserved in the aggregated AD.

The content's original USI will be transferred to and preserved in the separated ADs. Each content item will only exist in more than one AD if permitted by the USI, i.e. if the content was not bound to a single AD and Copies are allowed.

A CPCM Instance can be a member of only one AD at any time. A key point is that an Acquisition Point within a CPCM Device can bind CPCM Content to only one AD, if it is signalled in the Input Content that the content is to be bound to an AD.

The AD Management function supports commonly expected scenarios like device rental and borrowing, whereby the rented or borrowed device has access to CPCM Content bound to the host AD. The CPCM System ensures that the Authorized Usage of that content is not violated by the process of using the content with rented or borrowed CPCM Devices.

A detailed account of the expected functionality of the ADM component of the CPCM Instance within a CPCM Device is given in clause 7.3.5.

9 CPCM Usage Rules

9.1 General

A Usage Rule in CPCM is a particular operation upon, or behaviour of Content to be controlled within the scope of the CPCM System.

A complete set of Usage Rules assertions for a particular CPCM Content Item is referred to as the Authorized Usage of that CPCM Content Item.

A Content Item's Authorized Usage is expressed by its coding in Usage State Information (USI), which is thus CPCM Content metadata that signals the Authorized Usage for that particular Content.

The DVB CPCM Usage State Information Specification (TS 102 825-3 [i.5]) provides the definitive semantics for the USI. This clause of the Reference Model describes the basic control functions present in the DVB CPCM Reference Model to enforce the USI. USI in some cases maps explicitly and in others maps implicitly to the abstract CPCM Functions. A Content Item's USI may implicitly or explicitly inhibit one or more of the abstract functions (or sub-functions, described later) on that Content Item.

CPCM Usage Rules can be divided into the same groups used in TS 102 825-3 [i.5] to describe USI:

- Copy and Movement Control;
- Consumption Control;
- Propagation Control (both AD-based and Proximity-based);
- Output Control; and
- Ancillary Control.

The semantics of the USI for each of these Usage Rules are defined in the CPCM USI Specification (TS 102 825-3 [i.5]).

The following clauses describe the mapping of the CPCM Usage Rules to the abstract CPCM Functions described in the CPCM Reference Model.

9.2 Copy and Movement Control

CPCM Instances are required to implement the controls required to enable the following Content usage scenarios related to the Storage of Content Copies, wherever applicable to the CPCM functionality implemented:

- No restriction on Copying (Copy Control Not Asserted);
- Exactly one Copy is allowed to be made and maintained from the original Content Item (Copy Once). When the Copy is created, no further Copies are allowed (Copy No More), except for the temporary buffer as described for Copy Never;
- No Copies are allowed to be created (Copy Never), except for a secure temporary buffer Copy solely for the purpose of pausing of play-back, or trick-play. This buffer Copy will not be accessible to the user, will not be maintained longer than is necessary to provide the pause or trick-play function, and cannot be saved. A maximum duration of such a buffer Copy will be set by C&R regime;
- For Content emanating from systems or environments which provide their own pause and/or trick-play mechanism for the user, so any subsequent cascaded pause function within a CPCM Instance would be unnecessary and possibly cause confusion for the user (Copy Never, Zero Retention). This control could be applied in any of the following examples:
    - When it is required in order to comply with another CPS' requirements of CPCM as an authorized output from that system; or
    - When the Content source (for example a packaged media format or video-on-demand system) provides a mechanism for Pause that is realized outside of the CPCM System, prior to Acquisition. How that Pause function is actuated is outside the scope of the CPCM System; or
    - At the output of an existing temporary content buffer within the CPCM System for CPCM Content carrying the Copy Control State Copy Never or Copy No More, so that a further, cascaded time-shift buffer is inhibited.

The Move function for all legitimately made Copies implies the need to ensure that the original is removed, erased or made no longer accessible.

Copy and Movement Control relates to the CPCM Function of Storage, described further in clause 11.4.

9.3 Consumption Control

9.3.1 General

There are two aspects to Consumption Control foreseen in the CPCM System:

- Time-based usage (Consumption) of CPCM Content; and
- The ability to limit the number of concurrent Consumption and Export functions in operation for a CPCM Content Item.

9.3.2 Tethered Content

CPCM offers the possibility of being able to deliver content for Storage within CPCM that is not available for Consumption or Export until such rights have been Acquired from the CPCM Instance that has the ability to interact with the delivery system.

9.3.3 Time-based Usage

For CPCM Instances that are intended to offer access to such CPCM Content, it is required to implement the ability to enforce a signalled time window for the usage (Consumption) of that Content. This implies the need to keep track of time, i.e. to implement the Secure Time component of the Security Control part of the CPCM Instance (see clause 7.3.3.9). There are various modes of definition of the time window. It could be an absolute time window, or a specified period after Acquisition, or the first time the Content is Consumed, for example.

Time-based restrictions can apply to both the Consumption of CPCM Content and the Propagation Control Usage Rules, for example to provide for control of Remote Access in a flexible manner.

In practice this feature would need to be implemented in all CPCM Devices that have the facility to both Store and Consume CPCM Content, or to provide the Retrieved CPCM Content over a Device interface.

CPCM Devices that do not implement Secure Time would then not be allowed to Store any CPCM Content that had the time-based Usage Rule applied.

9.3.4 Concurrent Usage

For CPCM Instances that are intended to offer access to such CPCM Content, it is required to implement the ability to keep track of and limit the number of Consumption and Export functions in CPCM Instances that are active for a Live/Direct Content Item. If this restriction is activated for a given Content Item, the CPCM Instance inside the CPCM Device supplying the CPCM Content Item will grant access to the Content Item to CPCM Devices requesting to Consume or Export that Content until the signalled limit is reached. Any further requests for access to that Content Item will be denied. A buffer Copy of the content must not be able to circumvent the Concurrent Consumption Count.

9.4 Content Propagation

9.4.1 General

The Reference Model provides for Usage Rules to restrict the Propagation of CPCM Content inside the CPCM System to within certain realms, or to possibly leave the realms of the CPCM System altogether.

One of these realms is the Authorized Domain (AD), already described in clause 8. The other realms of propagation of CPCM Content are the Local Environment (LE), the Localized AD (LAD), and the Geographically-constrained AD (GAD).

The principle motivation for the AD as a CPCM Content Propagation realm is given in clause 8. The motivation for the other realms of Propagation restriction is mainly to control Remote Access to CPCM Content.

Remote Access is defined as access to CPCM Content from outside the Local Environment (clause 9.4.3), or the Localized AD (clause 9.4.4), in which that CPCM Content is made available, i.e. where it was Acquired, where it is Stored, or where it is being Processed.

Two example cases where Remote Access to CPCM Content could be controlled are:

1) To ensure that original broadcast footprints are not violated; indiscriminate Remote Access would imply its usage by those not intended to receive that Content in the original transmission.

2) To enforce regional black-outs of certain broadcast Content Items; in this case Content is intended not to be available within or outside of certain region(s) for at least a certain time.

The Geographic Area (GA) realm is considered for the purpose of enabling Remote Access to CPCM Content for CPCM Devices that are not present within the LE or LAD, but that happen to have the ability to verify their presence within the allowed Geographic Area.

The Remote Access Rule (RAR) applies to Content that is restricted to the LAD or GAD, as described in clause 9.4.4.

These Propagation realms are explained further in the following clauses.

Figure 17 shows the logical relationship between the various realms of Propagation Control defined in the CPCM System.

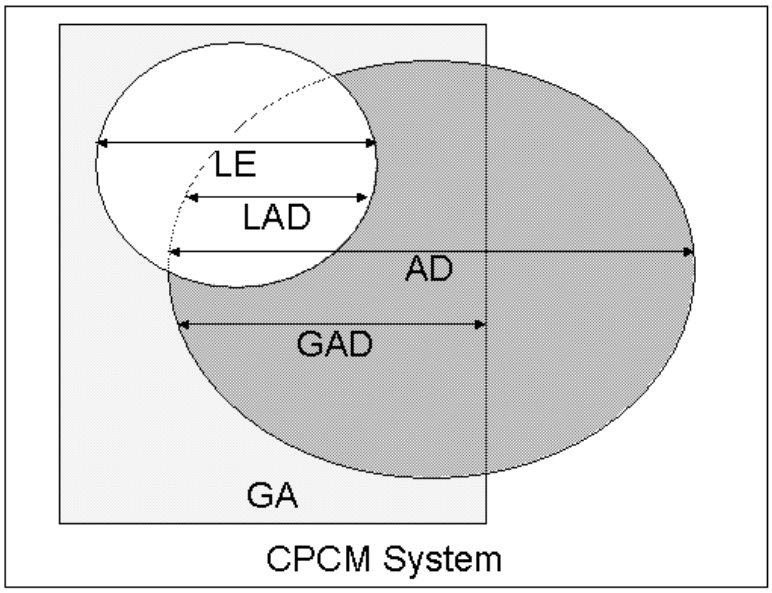

Figure 17: Logical Representation of Propagation Control Realms

Although the CPCM System will be the maximum realm of Propagation for CPCM Content, that is when the content is neither bound to an AD nor restricted to the LE, there is also a Usage Rule assertion to allow CPCM Content to leave the realm of protection of the CPCM System.

The following clauses describe the different CPCM Content Propagation realms in more detail.

9.4.2 Restrict to Authorized Domain

If Input Content carries the Usage Rule assertion that implies "Restrict to Authorized Domain", then that CPCM Content Item will be maintained within the CPCM System such that it is usable only by CPCM Devices belonging to the Authorized Domain in which it was first Acquired. In other words, it will be "bound" to that AD.

NOTE: A CPCM Device does not necessarily have to belong to an Authorized Domain, and even does not necessarily need to implement the capability to join an Authorized Domain. This does not necessarily mean that such a Device would not be able to use CPCM Content that is to be bound to an AD, but it may impact upon the scope of CPCM Content usage that would be allowed. In other words, certain CPCM Content usage implicitly does not violate the AD binding of the Content. One example of such usage would be the Consumption of Acquired CPCM Content on the same CPCM Device where the Acquisition takes place. The Storage of that Content on the Device would not violate the AD Usage Rule if that Content was not made available to other Devices, i.e. the Content is effectively bound to the Device as a surrogate for AD binding.

A CPCM Device that is not a member of the AD, or one that does not implement AD awareness, shall have access to AD-bound CPCM Content only for usage that does not violate the AD-binding. This is described further in clause 10.

Without any further Propagation restriction, CPCM Content with this Propagation rule asserted would be accessible for any CPCM Device in the same AD, wherever it happens to be located.

9.4.3 Restrict to Local Environment

The Local Environment (LE) is the immediate vicinity around a CPCM Device. It approximates to the physical extent of a home. The basic intention with the LE is to allow the Propagation of CPCM Content over the home (local area) network, without any AD binding, but to be able to prevent its Propagation over Wide Area Networks. This Usage Rule is orthogonal to the AD related Propagation restriction Usage Rules.

The Local Environment is not a CPCM property that is to be administered and managed. Rather, it is a dynamic ad-hoc property that is determined by a CPCM Device's location. All CPCM Devices in the immediate vicinity of each other are said to be in the same Local Environment. A CPCM Device shall implement a Proximity Test in order to be able to determine whether another device is Local to it or not. The intention is to allow the Propagation of CPCM Content within a local network but to prevent its Propagation over a wide-area network.

The technical method of determination of "in the immediate vicinity" is specified in CPCM System specification (TS 102 825-4 [i.4]). The Proximity Test might vary between the networking technologies that could be deployed in the CPCM System or there could be a common Proximity Test working at protocol layers above several different physical network interface layers.

The nature of the Local Environment becomes more apparent in Figure 18, where, when mapped to CPCM Devices, the Local Environment includes all CPCM Devices irrespective of their AD membership, and all CPCM Devices that are not a member of any AD or are just not AD aware, in the immediate vicinity.

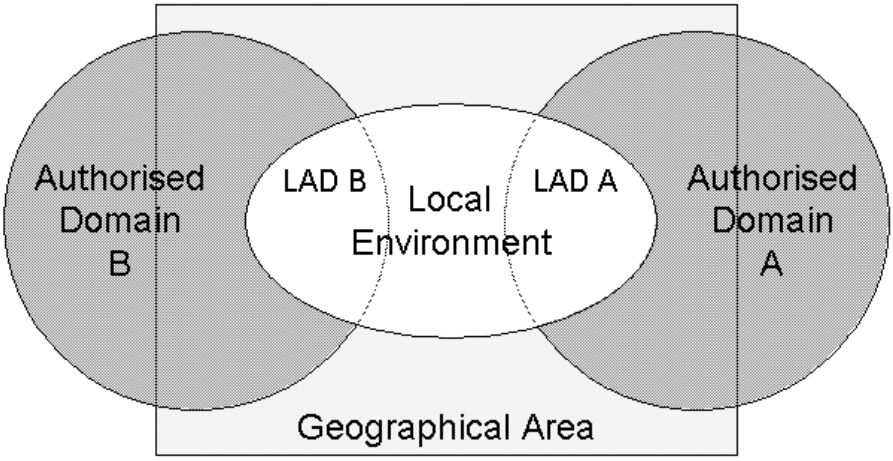

Figure 18: The Local Environment in relation to two ADs

The "Restrict to Local Environment" Propagation restriction is intended as a tool to control Remote Access to CPCM Content that is not bound to an AD.

9.4.4 Restrict to Localized Authorized Domain

The Localized Authorized Domain (LAD) is the logical interclause of the Authorized Domain and the Local Environment. In other words the LAD means all CPCM Devices that are in the Local Environment and that are also members of the same Authorized Domain. In practice this would mean all devices located within a home that also belong to that household, indicated by their membership in that household's Authorized Domain.

The Localized Authorized Domain, being the logical interclause of the Authorized Domain and the Local Environment, is naturally a subset of both. This is illustrated in Figure 19, based on the illustrative diagram used previously to depict the Authorized Domain.

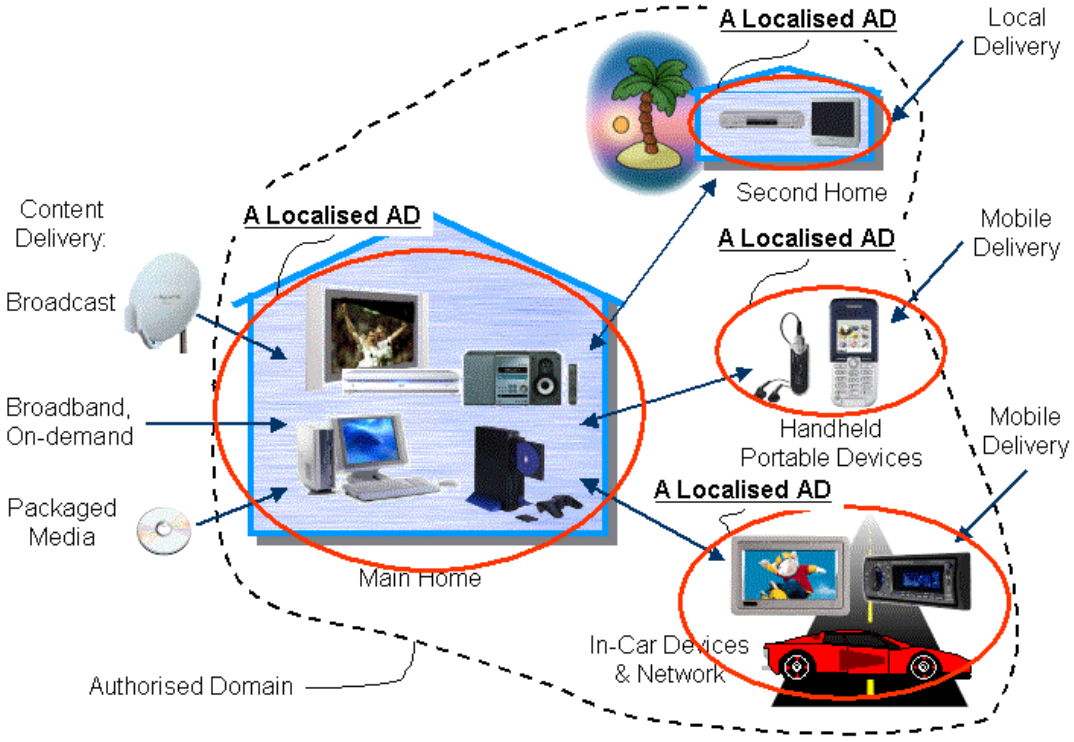

Figure 19: Localized ADs within an Authorized Domain

Thus, this example of an AD consists of the four indicated areas corresponding to Localized ADs - the main home, the second home, the portable devices carried on the person away from either home, and the in-car network when away from either home. When the mobile devices are carried inside the car, they are in the Localized AD of the car. When the mobile devices are carried back home, or the car is parked in the garage, the respective CPCM Devices are then within the Localized AD of the main home.

The purpose of the "Restrict to LAD" Propagation rule is to be able to control Remote Access to CPCM Content bound to the AD. In order to facilitate easy signalling of a temporary restriction of remote access, the Remote Access Rule provides a mechanism whereby such a restriction would expire after a certain time period or event. The expiration of the Remote Access restriction to a Copy of such a Content Item could be affected by any of the following:

- A signalled, or fixed, time period e.g. minutes/hours/days after Acquisition.
- Immediately after the recording of the Copy has been completed.
- On a fixed date/time.

The Remote Access Rule also applies to CPCM Content that is restricted to the Geographically-constrained AD (GAD), described in the next clause.

9.4.5 Restrict to Geographically Constrained AD

This aspect of Propagation Control within the CPCM System relates to the Geographic Area (GA). The CPCM System is not required to be able to explicitly control the Propagation of CPCM Content in geographic terms, nor is any CPCM Device required to be aware of its geographical location. Rather, the geographic Propagation restriction is intended as a special case for allowing Remote Access to CPCM Content that is otherwise restricted to the Localized AD when the CPCM Device performing the Remote Access does happen to have the facility of knowing its geographic location.

The logical interclause of the Geographic Area and the Authorized Domain is referred to as the Geographically-constrained Authorized Domain (GAD). The GAD is the set of CPCM Devices that are members of the same AD that happen to be located in the same GA. The devices need not be aware of the fact but some might be aware. Such awareness of presence in a GAD can be implicitly transferred to CPCM Devices that do not have this awareness by virtue of their presence within the Localized AD of the CPCM Device with geographic awareness.

The Local Environment is inherently a subset of any Geographic Area, and the Localized AD is inherently a subset of any Geographically-constrained AD (GAD).

9.4.6 Propagate to Untrusted Space

Certain types of CPCM Content may be allowed to leave the realms of the CPCM System altogether, i.e. to propagate into Untrusted Space.

This Usage Rule assertion could be suitable for content distributed according to the Creative Commons licence, for example, or could be valid for promotional clips of commercial content. This ability is included in the CPCM System because such Content could be included in a delivery channel that by default is a Trusted Input for CPCM, but for certain Content Items it might be desirable or necessary to allow such a free degree of Propagation.

This Propagation realm is included in the Output Control Usage Rule described in the next clause.

9.5 Output Control

As explained in clause 7.4, Device Outputs can convey different types of Content, namely CPCM Content (C.0), Consumed Content at a Consumption Output (C.2.2) and Exported Content (C.3). The abbreviated CPCM Content designations are explained fully under the treatment of each respective CPCM Functional Entity in clause 11.

The Output Control Usage Rule provides the ability to enable, disable or constrain particular CPCM Device Outputs for particular types of CPCM Content. The Output Control Usage Rule is applied to Outputs used for Consumption and Export.

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. Controlled Export/Output therefore subsumes both Export to a Controlled CPS and Output to a digital Consumption Output secured by a Controlled CPS.

CPCM Instances are required to implement the controls required to enable the following Content usage scenarios related to the Consumption and Export of CPCM Content, wherever applicable to the CPCM functionality implemented:

- Enabling and disabling of the Export of Content Items to Controlled CPSs;
- Enabling and disabling of the Output of Content Items to digital Consumption Outputs that are secured by a Controlled CPSs;
- Enabling and disabling of the Export of Content Items to Untrusted Spaces;
- Ability to enable and disable Analogue Export (C.3.4) that uses standard definition video formats for Content Items of the types necessitating this control;
- Ability to enable and disable the Output on C.2.2.2.SD Analogue Consumption Outputs for standard definition video for Content Items of the types necessitating this control;
- Ability to enable and disable Analogue Export (C.3.4) that uses high definition video formats for Content Items of the types necessitating this control;
- Ability to enable and disable the Output on C.2.2.2.HD Analogue Consumption Outputs for high definition video for Content Items of the types necessitating this control; and
- Ability to ensure that, if Image Constraint is signalled, a Content Item is passed through a Processing function that constrains the resolution of that Content Item prior to output of that Content Item on High Definition Analogue Consumption and Export Outputs for Content Items of the types necessitating this control. The constraining function is to be in accordance with the parameters specified in TS 102 825-3 [i.5].

For Output to Trusted CPSs (that are not Controlled CPSs) there are no per-Content Item Usage Rule controls.

Consumption and Export are treated further in clauses 11.6 and 11.7 respectively.

9.6 Ancillary Control

The CPCM System is required to provide a Usage Rule whereby protection via the CPCM Scrambler is not to be applied to Content within the CPCM System. This Usage Rule is referred to as "Do Not CPCM Scramble" (DNCS).

Thus for CPCM Instances that are intended to be able to handle such DNCS CPCM Content, it is required to implement the ability to ensure that a CPCM Instance does not invoke the CPCM Scrambler to scramble or encrypt that Content Item, if DNCS is signalled.

Content delivered in the clear from a Trusted Source without DNCS asserted must be protected by the CPCM System including CPCM Scrambling.

Further considerations regarding such DNCS CPCM Content are contained in clause 10.6.

See also clause 11.3.3 for further treatment of scenarios where this Usage Rule could apply.

10 CPCM Content

10.1 General

CPCM Content is content that is protected and managed within the CPCM System.

For the purposes of the CPCM Reference Model, CPCM Content is given the short-hand notation C.0. The various modes of CPCM Content described in this clause are given derivative labels of C.0 in the interest of brevity.

A Content Item is a discrete instance of Content of finite duration, for example, a TV episode, one segment from a news broadcast, a movie.

A CPCM Content Item in general consists of the Content itself plus its associated CPCM Content Licence.

The Content Licence is the set of CPCM metadata for that Content Item. A CPCM Content Licence is created for each item of Input Content at the Acquisition Point. It is described below in clause 10.2.

An informational representation of the USI may also be generated and inserted into the CPCM Content, if not already present prior to Acquisition. This inserted data describes the Content's Authorized Usage for informational purposes, for example for inclusion in an EPG or content discovery function, so that the user can be made aware of the Authorized Usage in advance. This information could use the same semantics and syntax as that used for USI, but of course the USI would typically be protected and contained in the Content Licence. The USI in the Content Licence is the definitive expression of the Authorized Usage.

CPCM Content can exist and be managed in various modes within the CPCM System. Which mode a particular CPCM Content Item assumes depends on several factors:

- The mode of CPCM Content tethering chosen by the content/service provider, or implemented in the particular Acquisition Point that Acquires that provider's Input Content.
- The chosen Propagation realm for the CPCM Content, for example there are potentially two different ways that CPCM Content can be managed if bound to the AD.
- Due to security constraints, certain USI states restrict the suitable modes of CPCM Content management.
- If the content provider chooses to apply the Usage Rule assertion of "Do Not CPCM Scramble" (DNCS, described in clause 9.6), then this obviously has significant implications about the level of security that can be provided by technical means, as well as allowing system-wide options as to the mode of management of such CPCM Content.

The first level of sub-classification of C.0 is thus:

- C.0.S, for Scrambled CPCM Content, the default mode; and
- C.0.C, for Clear CPCM Content, for the special case where DNCS is applied.

The CPCM Reference Model introduces various modes for how CPCM Content can exist and be maintained within the CPCM System. CPCM System specification (TS 102 825-4 [i.4]) defines how these modes themselves are managed, for example how CPCM Instances choose or negotiate CPCM Content modes upon exchanging or storing CPCM Content.

The Reference Model is agnostic with respect to the payload format of CPCM Content. Content format(s) are elaborated in TS 102 825-9 [i.9].

10.2 Content Licence

10.2.1 General

The Reference Model gives an overview of the contents of the Content Licence without stipulating its actual structure in detail. Figure 20 shows the logical constituent fields of the Content Licence, which may not need to be systematically populated.

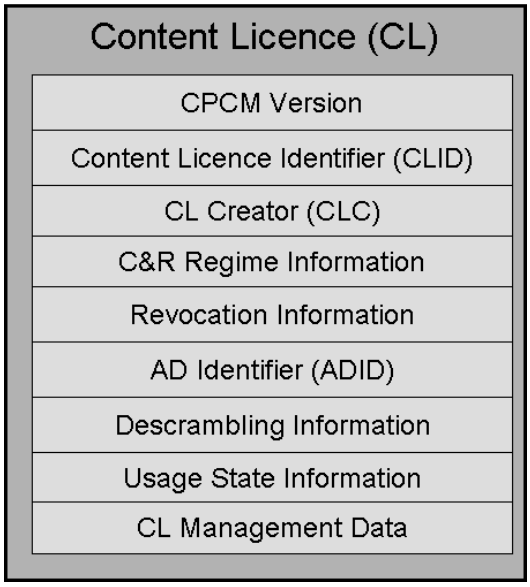

Figure 20: Notional Structure and Contents of the CPCM Content Licence

10.2.2 CPCM Version

This field gives the version of CPCM specifications applicable for the Content Licence.

10.2.3 Content Licence Identifier

The Content Licence Identifier (CLID) uniquely identifies the CPCM Content Licence.

The format of the Content Licence Identifier is specified in TS 102 825-4 [i.4].

10.2.4 Content Licence Creator

This field identifies the original creator of the (initial) Content Licence upon Acquisition into the CPCM System.

The content of the Content Licence Creator is specified in TS 102 825-4 [i.4].

10.2.5 C&R Regime Information

This field identifies a list of C&R regimes. A CPCM Instance shall implement at least one of them to access to the Content.

The format of the C&R Regime Information is specified in TS 102 825-4 [i.4].

10.2.6 Revocation Information

This field gives revocation information for each of the C&R regimes enable to access to the Content

The format of the Revocation Information is specified in TS 102 825-4 [i.4].

10.2.7 Authorized Domain Identifier

If the Content Item is bound to an Authorized Domain (AD), then the AD Identifier (ADID) indicates to which AD that Content Item is bound. If this field is zero, then the Content Item is not bound to an AD.

The generation of the ADID is specified in TS 102 825-7 [i.7].

10.2.8 Content Descrambling Information

This field contains relevant information to descramble CPCM Content: descrambling mode (see TS 102 825-5 [i.6]) and Content Descrambling Keys, that are the key(s) generated by the Key Management element of the Security Control part of the CPCM Instance that Acquired that Content Item into, or Processed that Content Item within the CPCM System. They are used by the CPCM Descrambling Tool to descramble the Content Item, when applicable.

For CPCM Content with the "Do Not CPCM Scramble" Usage Rule asserted this field is zero.

10.2.9 Usage State Information

The Usage State Information (USI) is the CPCM compliant coding of the Authorized Usage applicable to the Content Item associated with the particular Content Licence. The USI may also be carried embedded within the Content Item itself, but the USI stored in the Content Licence is the authoritative USI for that Content, with respect to its handling by CPCM.

The definitive set of CPCM USI is given by the CPCM USI Specification (TS 102 825-3 [i.5]).

10.2.10 Content License Management Data

Content License management data is any other data pertaining to the Content Item to which the Content Licence refers. It can be data necessary to achieve USI enforcement. It may be as well data for, and understood only by, a CPCM Extension, for example.

10.3 CPCM Content Licence Maintenance

10.3.1 General

For CPCM Content for which a Content Licence is maintained, there are two modes foreseen by which the CPCM Content Licence can be managed with respect to the Content Item:

- Separate or out-of-band Content Licence.
- Embedded or in-band Content Licence.

These modes are orthogonal to whether the CPCM Content is scrambled or not (C.0.S or C.0.C).

10.3.2 Out-of-band (Separate) Content Licence

This mode is when the Content Licence is securely stored and maintained by a CPCM Instance separately from the CPCM Content Item to which it refers. This type of CPCM Content is given the label C.0.O.

Figure 21 shows the representation of CPCM Content with out-of-band (separate) CL, with binding to the associated CPCM Content Item, used in subsequent diagrams to explain CPCM Content Management scenarios.

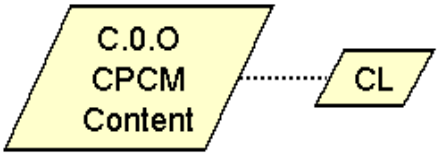

Figure 21: Depiction of CPCM Content with out-of-band (separate) CL

10.3.3 In-band (Embedded) Content Licence

This mode is when the Content Licence is embedded within the CPCM Content to which it refers. This type of CPCM Content is given the label C.0.E.

Figure 22 shows the representation of CPCM Content with in-band (embedded) CL, with binding to the associated CPCM Content Item, used in subsequent diagrams to explain CPCM Content Management scenarios.

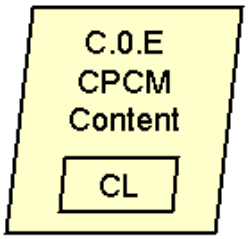

Figure 22: Depiction of CPCM Content with in-band (embedded) CL

10.4 CPCM Content Licence Protection

10.4.1 General

The CPCM System foresees several ways in which the Content Licence of any CPCM Content Item can be protected using the Security Toolbox (TS 102 825-5 [i.6]) as described in CPCM System specification (TS 102 825-4 [i.4]).

The security requirements for the storage of CL keys are the same in each of these modes of operation. All CL protection modes are applicable to both C.0.O and C.0.E.

The various CL protection modes are described in the following clauses.

10.4.2 CL Protection by SAC Session Key

In this mode, the CL is protected using the current SAC Session Key K_S.

CPCM Content protected in this mode is given the label C.0.SAC.

In order to introduce the basic schematic model of CPCM Content exchange between two CPCM Devices, Figure 23 shows the basic mode of C.0.O management inside and between CPCM Devices, as an example, when the CL is protected by K_S. This mode is just as valid for C.0.E.

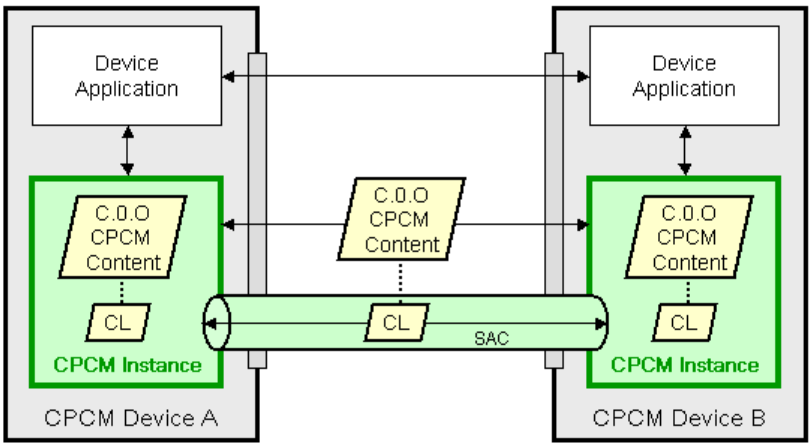

Figure 23: Generic model of C.0.O Storage, and CL transfer protected by SAC

For this method, the following logical steps have to be taken before a CPCM Content exchange between CPCM Instances can take place:

1) the Source CPCM Instance verifies the Content Licence integrity and that the content transfer or usage will not violate the Authorized Usage given in the Content Licence; and

2) the CPCM Instances establish trust.

The following logical steps have to be taken in addition when the Content Licence needs to be exchanged from the Source CPCM Instance to the Destination CPCM Instance:

1) A SAC is established between the CPCM Instances.

2) The Source CPCM Instance transfers the Content Licence to the Destination CPCM Instance.

3) The Destination CPCM Instance verifies the Content Licence integrity and enforces the Authorized Usage given in the Content Licence.

The depiction of Stored C.0.O inside the CPCM Instance means that the CPCM Instance ensures the security of the CL, not that C.0.O and the CL are physically Stored inside the CPCM Instance. As explained in clause 7.5, physical storage is assumed not to be secure in itself, but that the CPCM Instance managing that CPCM Content does so in a secure manner.

When C.0.O is transferred between two CPCM Devices, the Content Licence is transferred separately in the SAC between the two CPCM Instances, i.e. for transfer the CL is always protected with the SAC session key. The C.0.O Content passes over the network interface, encrypted with the CPCM Scrambler key(s) carried in the Content Licence.

10.4.3 CL Protection by Device Secret

In this mode, the CL is protected using a permanent Device Secret Key K_D known only to the CPCM Instance inside the respective CPCM Device.

CPCM Content protected in this mode is given the label C.0.D.

This mode is valid only for the Storage of CPCM Content managed by the CPCM Device, as such device secrets shall not be divulged to any other entity.

The choice of this mode in a CPCM Device implementation enables CPCM Content Acquired and Stored by that Device to retain full control over that Content.

10.4.4 CL Protection by AD Secret

In this mode, the CL is protected using a permanent Authorized Domain (AD) Secret Key K_{AD} accessible only to the CPCM Instances inside the CPCM Devices that are members of that AD.

K_{AD} is equivalent to the AD Secret (ADS) described in clause 7.3.3.2.4.

CPCM Content protected in this mode is given the label C.0.A.

This mode is valid both for the Storage and transfer of CPCM Content within the CPCM System. It enables the sharing of CPCM Content within an AD without the need for member CPCM Devices of the AD to continually establish a SAC for the exchange of CPCM Content.

10.5 CPCM Content Security

There are anticipated to be many other issues to be addressed in connection with the three CL protection modes in connection with particular CPCM Usage Rule assertions or combinations thereof.

An exhaustive analysis of such is given in CPCM System specification (TS 102 825-4 [i.4]).

10.6 CPCM Clear Content

The default protection mode for CPCM Content is to apply all the CPCM security tools, i.e. that CPCM Devices establish mutual trust before transferring CPCM Content that is protected by the CPCM Scrambler and used in accordance with the secure USI contained in the Content Licence.

CPCM is however required to provide the facility to manage Content that is to be maintained within the CPCM System explicitly without the application of the CPCM Scrambler as a tool for protecting that Content. This type of Content is referred to as CPCM Clear Content and is given the label C.0.C.

C.0.C results from the assertion of the "Do Not CPCM Scramble" (DNCS) Usage Rule in the Input Content, described in clause 9.6. CPCM Clear Content is content that has DNCS set upon Acquisition, directing subsequent downstream CPCM devices to not CPCM Scramble the Content.

DNCS is intended to apply to both transmission of CPCM Content between CPCM Devices and to the storage of CPCM Content.

There may be circumstances where non-CPCM encryption is applied. In all circumstances of Authorized Usage, such application of encryption shall be transparent to users of CPCM Clear Content.

The application of DNCS by the content provider is independent of whether the content is delivered in the clear or protected by scrambling. Content delivered in the clear will not necessarily be Acquired as CPCM Clear Content.

There may also be CPCM System-wide options regarding the appropriate and sensible level of security to be applied to other aspects of the management of CPCM Clear Content and the respective Content Licences within the CPCM System. CPCM Instances inside CPCM Devices that are known to only ever have access to CPCM Content where the DNCS Usage Rule is asserted might not need to implement all aspects of the CPCM Security Control components listed in clause 7.3.3, for example Trust Establishment and SAC Management.

The actual requirements for such CPCM Devices are laid down by CPCM specifications and C&R regimes.

CPCM Devices are nevertheless required to honour all applicable Authorized Usage signalled in the USI in the Content that these Devices are able to handle. A CPCM Device that acts as a Sink for CPCM Content must implement all CPCM security tools and mechanisms required for the intended usage of that Device, otherwise interoperability with all CPCM Content Sources will not be given. This applies whether to content is marked DNCS or not.

10.7 CPCM Content Item Delineation

There is no secure mechanism for delineating service events that are intended to become different Content Items once Acquired by the CPCM System. This is not an issue for on-demand type content delivery systems or with Content from a storage medium, where the Content is made available as separate items at source, but with a continuous stream of content containing concatenated service from a typical broadcast source there may be concerns around securing the termination of one event (Content Item) having a certain Authorized Usage, to the next event (Content Item) having a different Authorized Usage.

Signalling of the delineation of service events is typically the responsibility of the transport mechanism that delivers the content to the Acquisition Point and thus outside the scope of CPCM. The delivery system shall signal delineation of service events to the Acquisition Point as described in TS 102 825-4 [i.4].

10.8 CPCM Content Revocation

If a CPCM device has been compromised, e.g. cloned, it may be revoked on a per Content Item basis. Compliant CPCM Devices, including those that do not use on-line authentication, will be capable of being denied specific CPCM Content in accordance with a Certificate Revocation List (CRL).

The CPCM Instance should include the facility to explicitly inform the user when such a revocation takes place, as one of the foreseen standard CPCM notifications to the CPCM Device's host application, via the CPCM Interaction interface, described in clause 7.2.3.

The CPCM Content revocation method(s) and CRL are specified in CPCM System specification (TS 102 825-4 [i.4]).

10.9 CPCM Content Recovery

Facilities to enable the user to recover legitimately obtained CPCM Content in the case of damaged CPCM Devices of components thereof, or when upgrading or through the replacement of components of CPCM Devices are out of scope of the CPCM System. But the CPCM System shall not preclude the provision of such facilities by CPCM Device manufacturers or CPCM Content providers.

11 CPCM Content Management

11.1 General

This chapter combines all the previously described concepts in order to provide the generic CPCM Content Management model.

Each of the five abstract CPCM Functional Entities are described in terms of their mapping to actual implementations in CPCM Devices and the foreseen content management scenarios.

11.2 Basic Content Management Model

The CPCM System provides a platform for interoperable post-delivery content management and protection, including a common set of Usage Rules for all content within the CPCM System.

This basic content management model is shown in Figure 24.

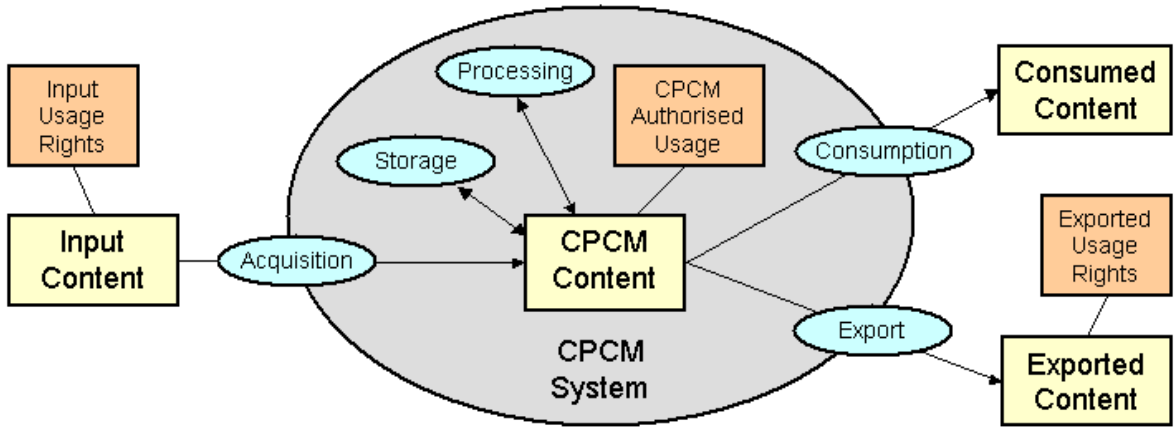

Figure 24: Basic Content Management Model

Input Content, with its associated input usage rights, is Acquired by the CPCM System to become CPCM Content, with its associated CPCM Authorized Usage. Thus every channel of content Acquisition into CPCM must have a mapping of that channel's set of Usage Rules to the common CPCM Usage Rules.

While within the CPCM System, CPCM Content can be Stored or Processed in accordance with the Authorized Usage associated with the content.

CPCM Content leaves the CPCM System when it is Consumed, or Exported from the CPCM System. Both of these operations might also be affected by the content's Authorized Usage.

The following clauses describe each of the abstract Functional Entities in terms of all aspects of content management, including break-downs of the different content types, critical issues regarding content management itself in each case, and mappings of each Functional Entity to more real-world CPCM scenarios.

11.3 Acquisition

11.3.1 General

Input Content is received from a Trusted Source and ingested into the CPCM System at the Acquisition Point. Figure 25 shows this, extracting the relevant part of the Abstract Model, and expanding it showing the different types of Input Content.

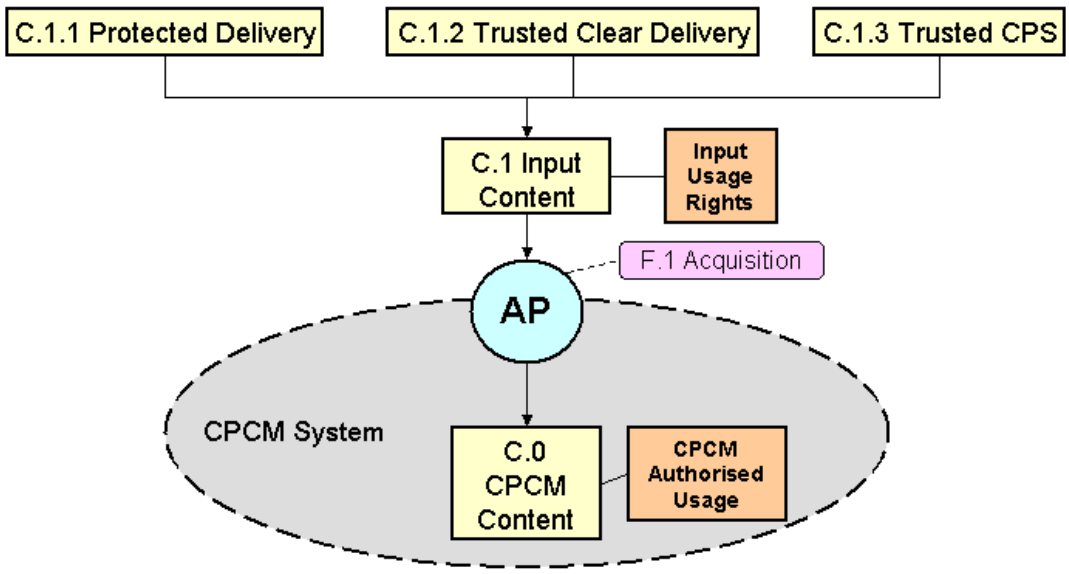

Figure 25: Input Content

"Trust" between the Trusted Source and the CPCM Instance Acquiring the Input Content is based on compliance, with both the Trusted Source and the CPCM System, under the control of C&R regime. In some cases this trust might be established explicitly by technical means, for example with a DRM system over the internet, but this trust establishment is outside the scope of the CPCM System.

The CPCM Reference Model does not foresee the Acquisition of Content from analogue inputs.

Figure 26 shows the generic logical model of the Acquisition Point and the process of Content Acquisition. The Acquisition Point performs the transfer of content from the delivery system or Trusted Source as well as the generation of CPCM USI for that content based on the Input usage rights. This is shown for the example of the generation of C.0.O in the CPCM System.

As shown in FigureS 25 and 26, there are three kinds of Input Content for CPCM that together comprise the Trusted Sources for Acquired Content. Each has different methods of trust establishment with CPCM, and in the case of Trusted Clear Delivery two security models are foreseen, as already described in clause 10.6.

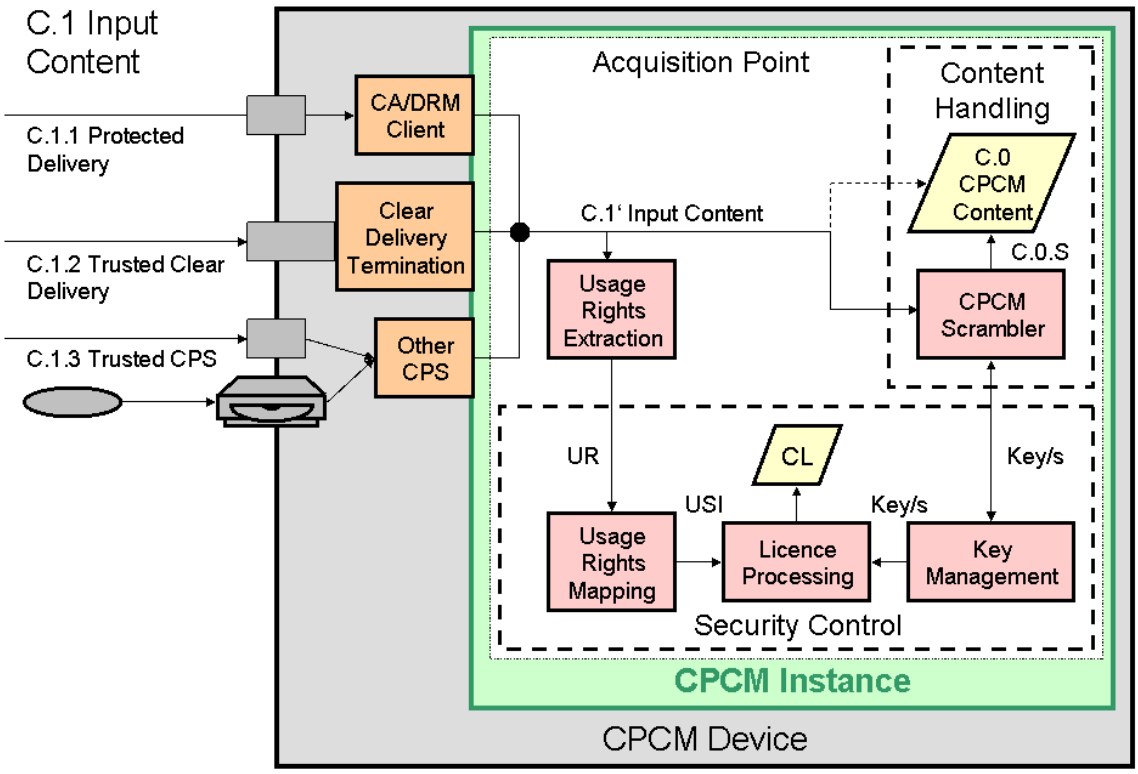

Figure 26: Generic Logical Model of the Acquisition Point and Content Acquisition

11.3.2 Protected Delivery

11.3.2.1 General

Input Content from a protected delivery system or channel is handed over securely to the CPCM Instance by the Protected Delivery Client. If the Content is already delivered with CPCM compliant scrambling applied and the keys are available to be propagated in the CPCM system, then that content will not need to pass through the CPCM Scrambler, but a Content Licence might need to be generated by the Licence Processing component of Security Control, if it is not already present (e.g. embedded in the Content, C.0.E, as described in clause 10.3.3).

Mutual trust with CPCM for content handover can be established in two ways:

- Under C&R regime, whereby the respective protected content provision system (e.g. CA or DRM system) has attained mutual approval for content exchange with CPCM (e.g. CPCM is an approved output of the DRM system).
- Via a CPCM Extension that mutually establishes trust with the CPCM Instance (see clause 12).

11.3.2.2 Conditional Access Integrated in the CPCM Device

In this mode of Protected Delivery, the proprietary Protected Delivery Client is fully integrated inside the CPCM Device. This is depicted in Figure 27.

Here the complete process of content Acquisition from the CA system takes place within an integrated host device, e.g. a Set-Top Box (STB). The Protected Delivery Client performs the secure transfer of C.1.1 to the CPCM Instance.

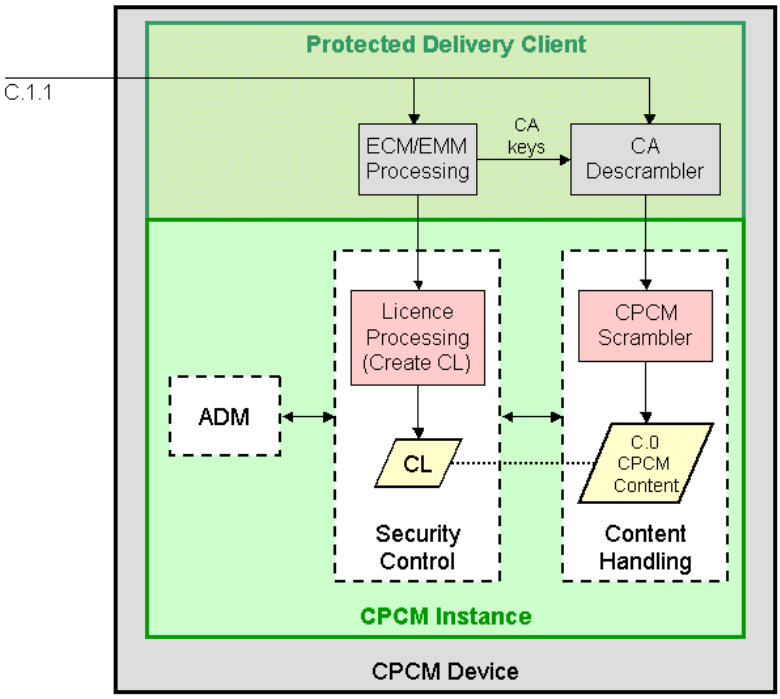

Figure 27: Integrated-CA Acquisition

11.3.2.3 Conditional Access Smart-Card

Here, two example models are depicted whereby smart-card based approaches could implement the Acquisition of Protected Delivery Content into the CPCM System.

The first is where part of the CA Protected Delivery Client is hosted in the smart-card.

In the first example, Content Acquisition takes place in a vertical market set-top-box (STB) where the Protected Delivery Client is usually implemented in part in the smartcard as the core CA client, in part in the STB as the CA kernel. The Protected Delivery Client is responsible for feeding the CA descrambler with the CA-controlled content keys (Control Words) and also controls the use of the Content in the STB (e.g. DVR recording and playback control in association with CA-controlled rights). This Protected Delivery Client will therefore also be responsible for controlling the handing over of Content to CPCM, generating the associated Content Licences, and renewing them at a later stage, whenever applicable, due to being identified in the Content Licence Creator field in the Content Licence. The interface between the Protected Delivery Client and the CPCM Instance does not need to be specified by CPCM for the sake of interoperability, but will be subject to C&R regime.

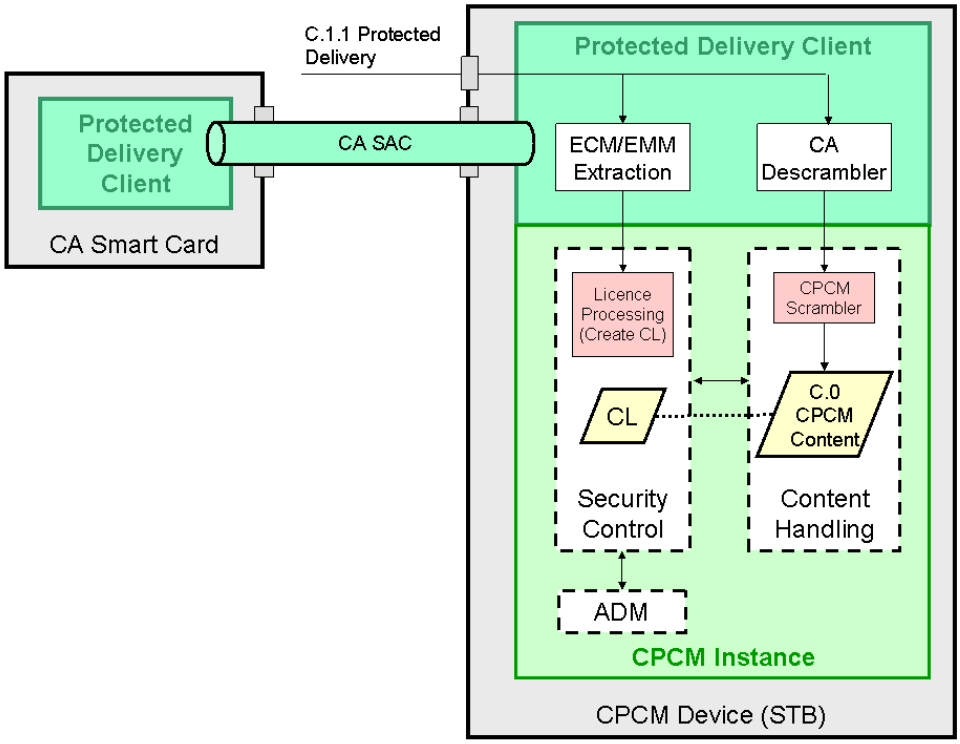

Figure 28: Smart-Card Based Acquisition Example 1

In the second kind of smart-card based CPCM protected delivery receiver the smart-card itself hosts at least a part of the CPCM Instance, usually the Security Control part, and this builds a SAC with the CPCM Instance located in the host protected-delivery receiver device. An example implementation of this mode is shown in Figure 29.

In this mode of Protected Delivery, the CPCM functionality implemented in the CA Smart Card has the task of generating CPCM Content Licences for the Acquired Content, but does not perform the Content Handling functions. These are performed in the CPCM Device, which must also implement a particular part of the proprietary Protected Delivery Client.

In this example the implementations of Security Control use the CPCM SAC between the smart card and receiver to deliver the CA keys to the CA descrambler in the host. This can be done by appending private data; in this case the CA keys, to CPCM Communications, in this case the Content Licence, as part of the Auxiliary Data, whereby the CPCM Instance implementation knows how to handle this private extension data. This is essentially an example of a CPCM Extension in the logical model.

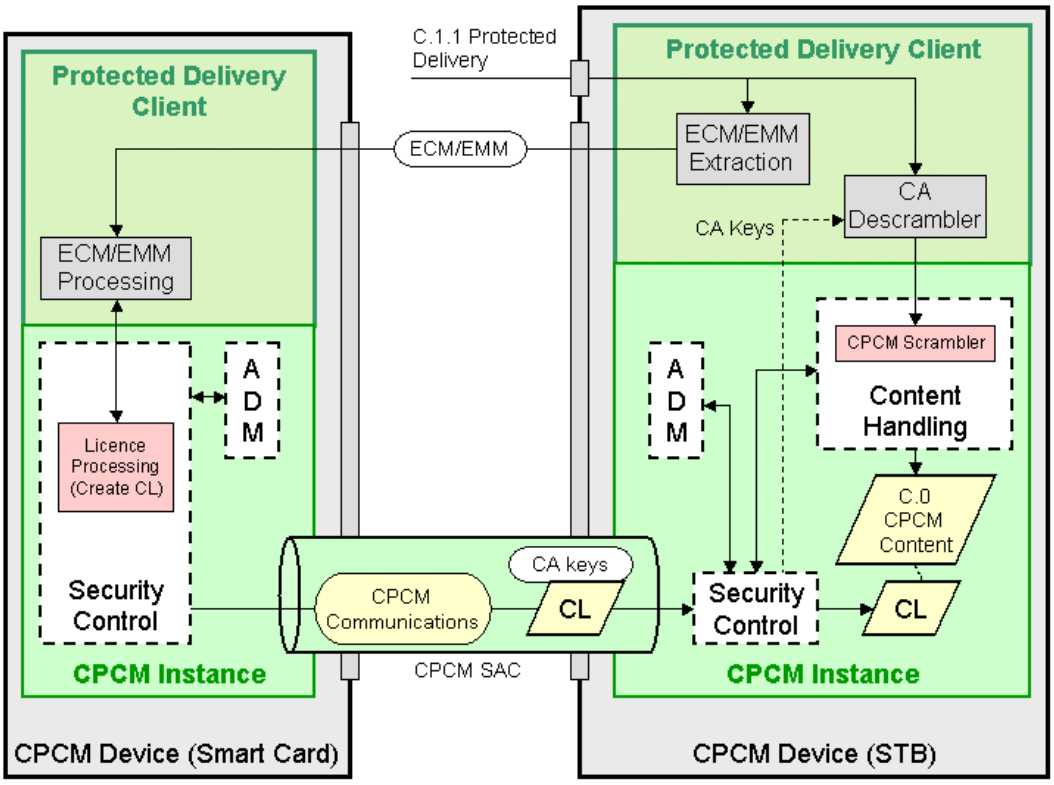

Figure 29: Smart-Card Based Acquisition Example 2

11.3.2.4 Conditional Access Module

This form of Acquisition is realized in CPCM by implementing two independent and compliant CPCM Instances, one in the Conditional Access Module (CAM) and one in the generic host receiver Device, which needs no content-provider or CA system specific functionality.

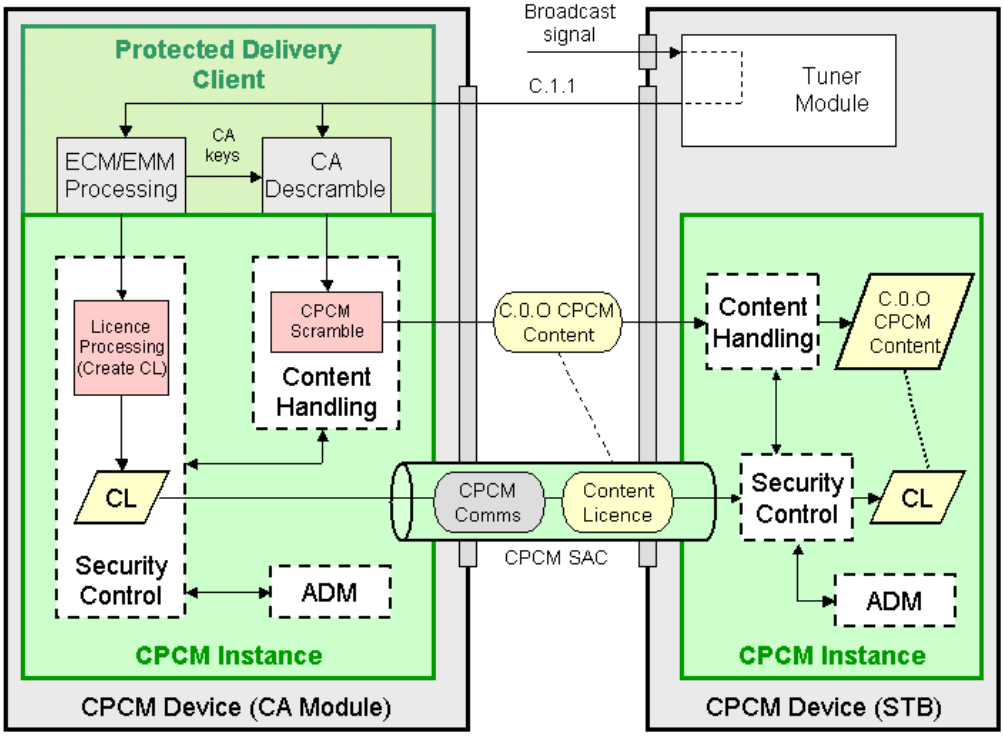

Figure 30: CA Module Based Acquisition Example

The CA Module performs the handover of CA-protected content to CPCM. It passes back protected CPCM Content to the- host device. The host device needs to have no CA-specific functionality, and the content flow from the CA Module to the host device is protected by CPCM. The example shown above assumes Separate or Out-Of-Band CL mode, as described in clause 10.3.2.

Such a physical interface could be either one that is used as a generic home network interface, or a more specific dedicated physical interface, like the DVB Common Interface. In this case this mode of operation effectively solves the problem of the unprotected DVB Common Interface return path.

11.3.2.5 Free-To-View Delivery

Free-To-View (FTV) delivery is where the broadcast delivery of the Content is protected by scrambling. This clause describes the special case of FTV where this Content is intended to become CPCM Clear Content (see clause 10.6) after Acquisition into the CPCM System, by application of the Ancillary Control Usage Rule of "Do Not CPCM Scramble" (see clause 9.6). In the other case, where this Usage Rule is not asserted, this delivery model would be the same as that described in the previous clauses.

Figure 31 depicts this case as an example when only the Licence Processing component of Security Control, which creates secure Content Licences for the CPCM Clear Content Acquired by the receiver, is required.

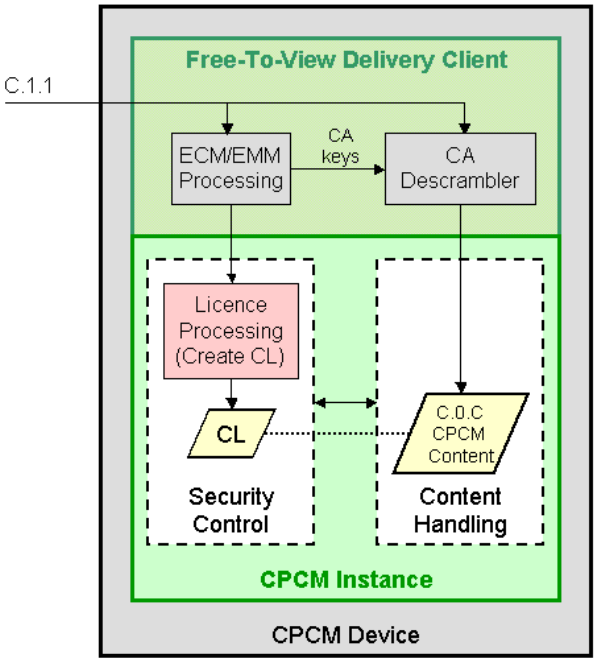

Figure 31: Acquisition of Free-To-View Example 1

The handling of CPCM Clear Content was described in clause 10.6. Applied to the case of Free-To-View Acquisition, the CPCM Scrambler will not be activated. Figure 32 shows the example of the generation of embedded-CL CPCM Content where Proximity Control is applied in Security Control.

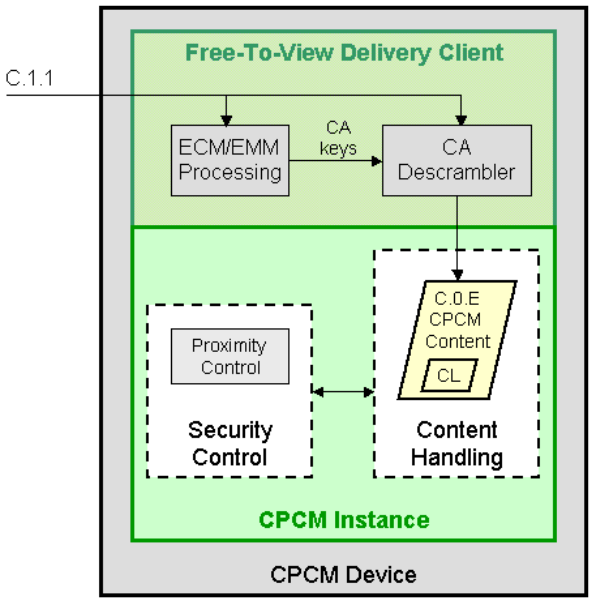

Figure 32: Acquisition of Free-To-View Example 2

11.3.2.6 DRM System

The DRM System form of Acquisition is exemplified below in Figure 33. Here the DRM system client transfers Content to the CPCM Instance by translating the DRM system licence and usage rights into a CPCM Content Licence containing the mapped CPCM Authorized Usage for the respective Content Item. This example assumes C.0.O is generated.

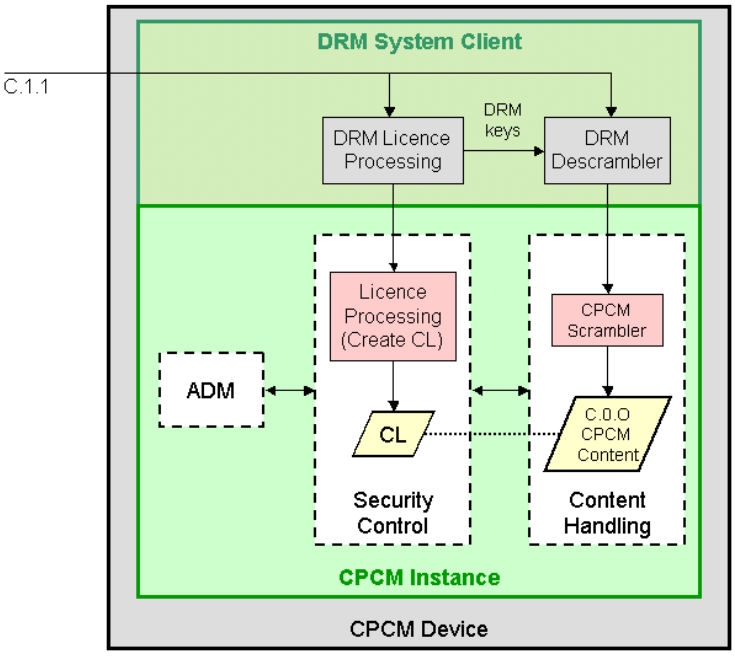

Figure 33: Acquisition from DRM System, Example 1

A second example of Acquisition from a DRM system, Figure 34, shows the case where the DRM system delivers the Content Item wrapped in a container and the DRM system client unwraps the container to enable the CPCM Instance implementation to generate a CPCM Content Licence and CPCM Content in much the same way as in the first example.

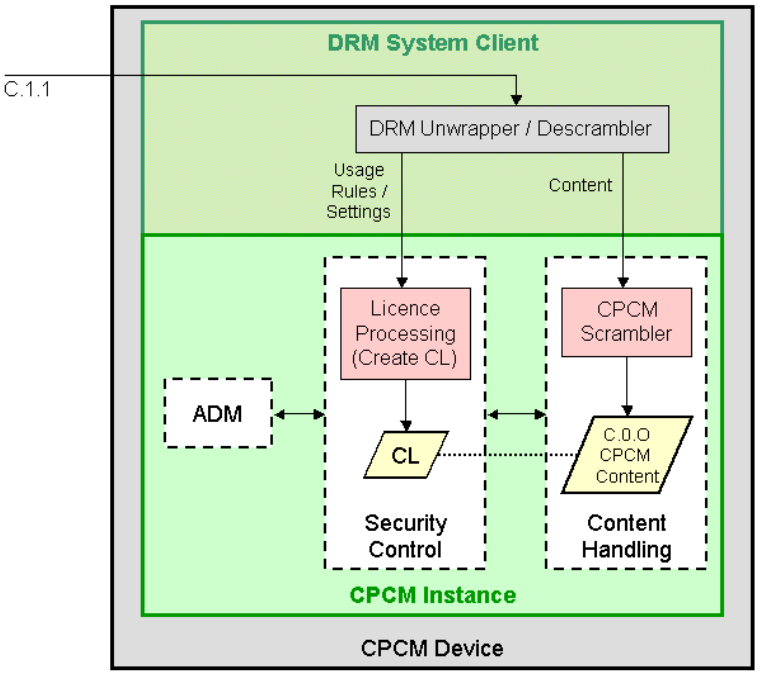

Figure 34: Acquisition from DRM System, Example 2

A variation of either example could be that the DRM system deploys the same Content Scrambling cipher and mode as the CPCM System and the keys are available to be propagated in the CPCM system, so possibly avoiding the need to descramble and re-scramble the Content Item upon Acquisition in the CPCM System. This is depicted in Figure 35.

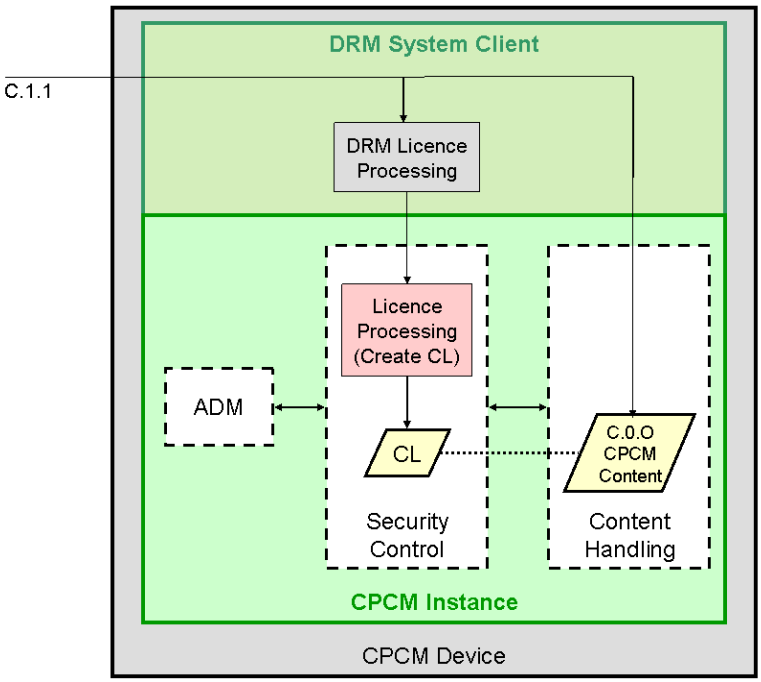

Figure 35: Acquisition from DRM System, Example 3

11.3.3 Trusted Clear Delivery

This is clear, meaning unprotected, Input Content from a Trusted Source. A Trusted Source for clear content could be, for example, a broadcast tuner or broadband terminator (CPE). The clear-to-air tuner module that tuned and decoded a signal that could only be generated by a "commercial" broadcaster could be trusted implicitly by virtue of its robust physical connection within a CPCM Device. This Content has associated Input usage rights, from which the appropriate USI will be mapped upon Acquisition.

As explained in clause 10.6, one model for Input Content delivered in the clear will be that it is required that CPCM also maintains such CPCM Content in unscrambled form, i.e. CPCM Clear Content, signalled with the DNCS Usage Rule asserted.

A possible scenario for such a receiver is a variation of that described in Figure 32, depicted here in Figure 36. Here the broadcast tuner module is classed as a Trusted Source for clear-to-air delivered Input Content.

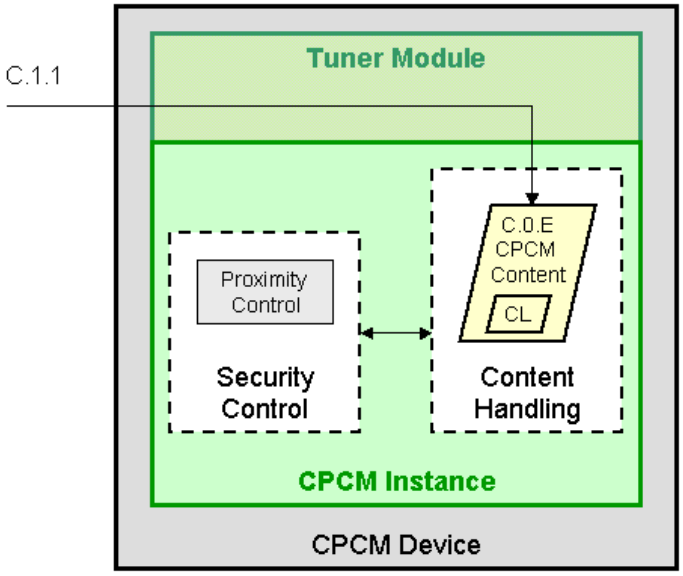

Figure 36: Acquisition of CPCM Clear Content Example

11.3.4 Trusted Content Protection System

A Trusted Content Protection System (CPS) is a third-party content protection system with which a predetermined set of CPCM interoperability rules, including a USI mapping, has been defined and approved by, for example, a C&R regime.

This form of Acquisition is shown in Figure 37 for the case of C.0.O generation in CPCM.

Any trust establishment between a CPS system and CPCM is not necessarily reciprocal. For example, a CPS might include CPCM as a Trusted Output and CPCM has the CPS as a Trusted Input but that does not mean that CPCM automatically includes that CPS on the list of Trusted Outputs (CPCM Export, see also clause 11.7).

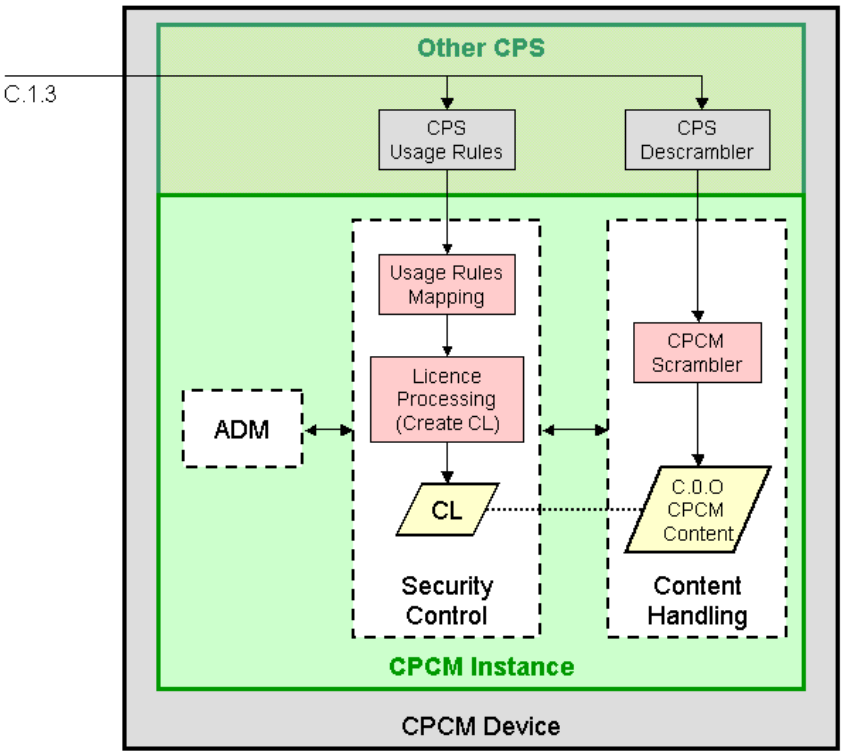

Figure 37: Acquisition from Trusted CPS

11.4 Storage

Subject to USI allowing a Copy to be created, the Copy of a piece of CPCM Content that is stored in a Storage Entity is referred to as CPCM Stored Content (C.0.2). When a Content Item is copied or consumed, if allowed by the USI, then that Content flow from the Storage Entity is referred to as Retrieved Content (C.0.3). Figure 38 shows this, extracting the relevant part of the Abstract Model.

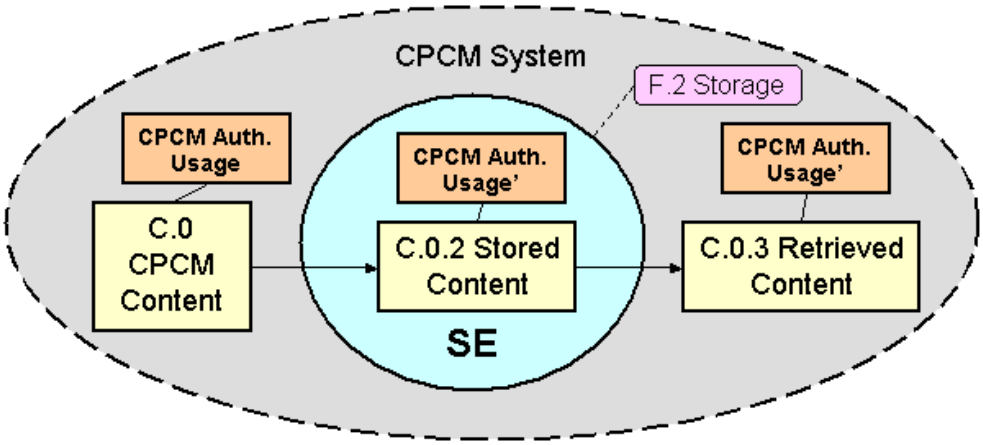

Figure 38: Stored and Retrieved Content

The Storage Entity is an abstract Functional Entity that is inside the CPCM Instance hosted by a CPCM Device. Physical storage drives and storage media are themselves outside the CPCM Instance. The Storage Entity handles CPCM Content that is stored on physical storage. Storage is generally either fixed and/or embedded in the CPCM Device, or removable media that are read or written in a storage drive in the CPCM Device. As mentioned in clause 7.5, there is no distinction between fixed and removable physical storage for the purposes of the Reference Model, in that the Storage Entity inside the CPCM Instance treats them in the same way logically.

Figure 39 shows the generic logical model of CPCM Content Storage, depicting the Storage Entity in relation to Device interfaces and example storage drives. Only the CPCM A.P.E.C.S. Content Handling functionality is depicted here, because there is no interface to or from outside the CPCM System involved with Storage. The only operation on Content Licences associated with Storage is when a new Content Licence is created for a newly created instance of a Content Item that is allowed to be Copied.

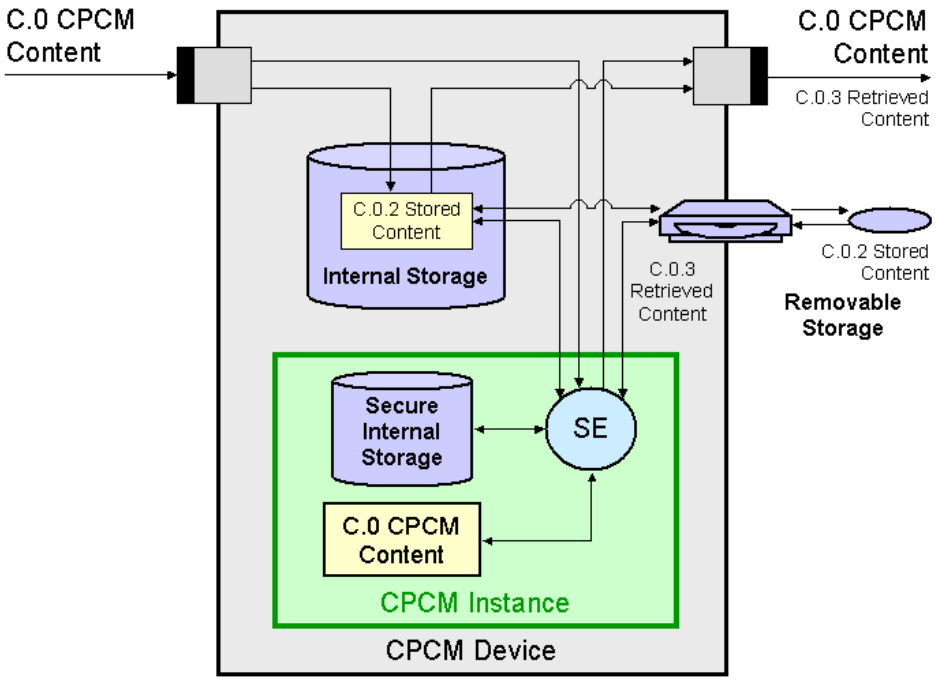

Figure 39: Storage Entity, Device interfaces and storage drives

Figure 39 effectively combines all the different kinds of Storage possible in CPCM. The following describes each type in more detail, clarifying the mapping of the logical model to real-world examples of storage devices.

If allowed by the USI (Copy Control Usage Rule assertion for that Content), the Storage Entity creates the Copy (C.0.2 Stored Content) from CPCM Content being input at the CPCM Device's interface(s), from CPCM Content being handled inside the CPCM Instance, or from an existing Stored Content Item being handled in a storage drive (fixed or removable) in the CPCM Device hosting the Storage Entity.

Retrieved Content can be output at the Device's CPCM Interface(s) when being exchanged with other Devices within the CPCM System.

The Storage Entity can Retrieve Stored Content from fixed or removable Storage Media, or from the Device's Input Interface(s), for further handling inside the CPCM Instance.

From Figure 39, it is evident that a storage device that has no other function than to offer physical storage capacity for CPCM Content does not need to even implement a CPCM Instance. All CPCM Content that it stores is protected, as far as required by its USI, thus only compliant CPCM Devices are able to access such CPCM Content. CPCM Content is always stored and retrieved under the control of other CPCM Devices. This kind of storage device can also be referred to as a "dumb bit bucket". If the storage device implements any CPCM Functional Entity in addition to Storage, then this must be done, as always, inside a CPCM Instance inside the device.

Storage is directed by the Copy Control USI. For Content carrying the Copy Control state Copy Never or Copy No More, no static instance, or Copy, shall be created by the Storage Entity. For CPCM Content with Copy Control state Copy Once, the resulting Copy (Stored Content in the Storage Entity) shall carry the Copy Control state Copy No More (CNM). For CPCM Content with Copy Control state Copy Control Not Asserted (CCNA), the resulting Copy (Stored Content) shall also carry the Copy Control state Copy Control Not Asserted.

The Move function is a facility that can be provided by any CPCM Device implementation. Any such Content Move functionality must of course comply with Copy Control and Propagation Restriction USI. For Copy Control this means that when the Content Item Copy carries a Copy Control Usage State of Copy No More (Copies should never exist with the Copy Control Usage State of Copy Never), then the original is no longer accessible once the Moved Content Item has been created.

11.5 Processing

Processing in the context of CPCM is a CPCM compliant operation upon, or Authorized Usage of Content whereby CPCM Content undergoes a permitted transformation from its original form to create new transformed CPCM Content. Figure 40 shows this, extracting the relevant part of the Abstract Model for Content classification.

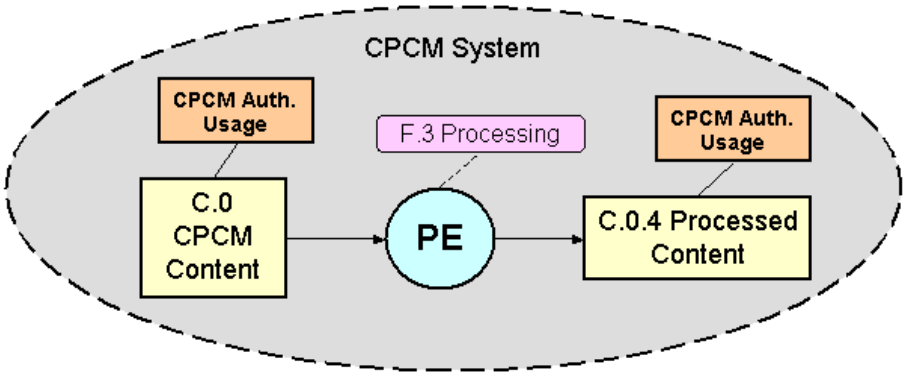

Figure 40: Processing

Examples of Processing functions could be:

- Transcoding to a different compressed format, video resolution or frame rate, or audio sampling rate.
- Application of audio/video effects.
- Insertion of alternate data or content components.
- Extraction of still images from a video stream.

Figure 41 shows the logical diagram of all options with a Processing Entity, based on the example of C.0.O.

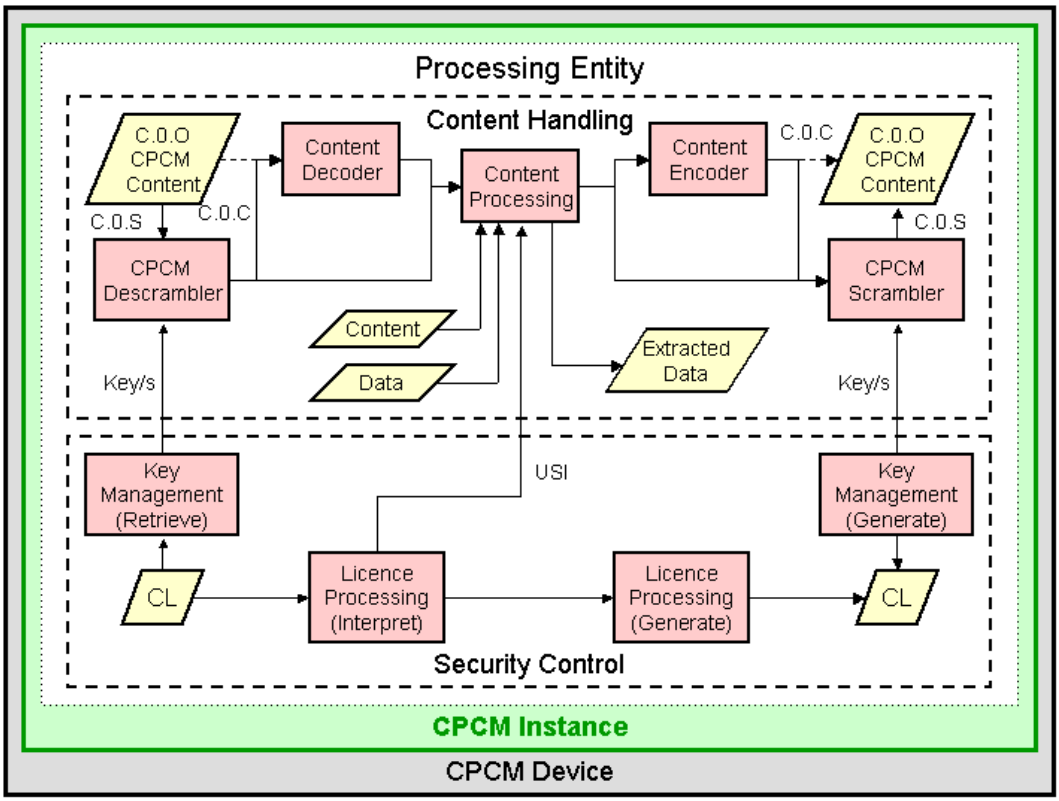

Figure 41: Processing Entity

It could be defined under compliance rules as to which of these are allowed generally, or it could be stipulated that some are allowed in conjunction with, for example, Copy Control USI states. The definitive rules are defined by each C&R regime.

11.6 Consumption

11.6.1 General

Consumed Content is elaborated in order to differentiate between pure sound and vision and, for example, electrical and optical device outputs that are constrained to provide only the functionality of immediate Consumption by a connected device. Figure 42 shows this, building on the relevant part of the Abstract Model for Content classification.

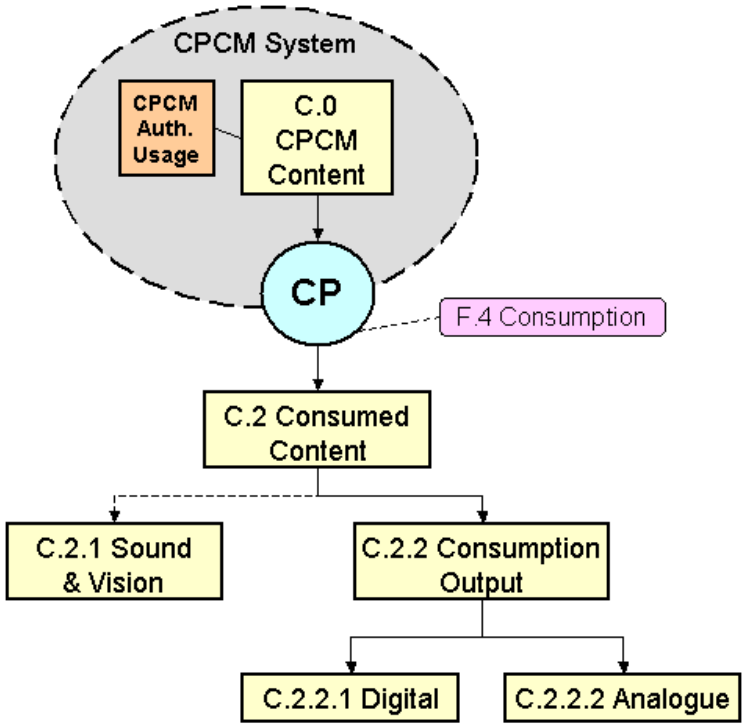

Figure 42: Consumed Content

Figure 43 shows the logical model of the Consumption Point, based on the example of C.0.O.

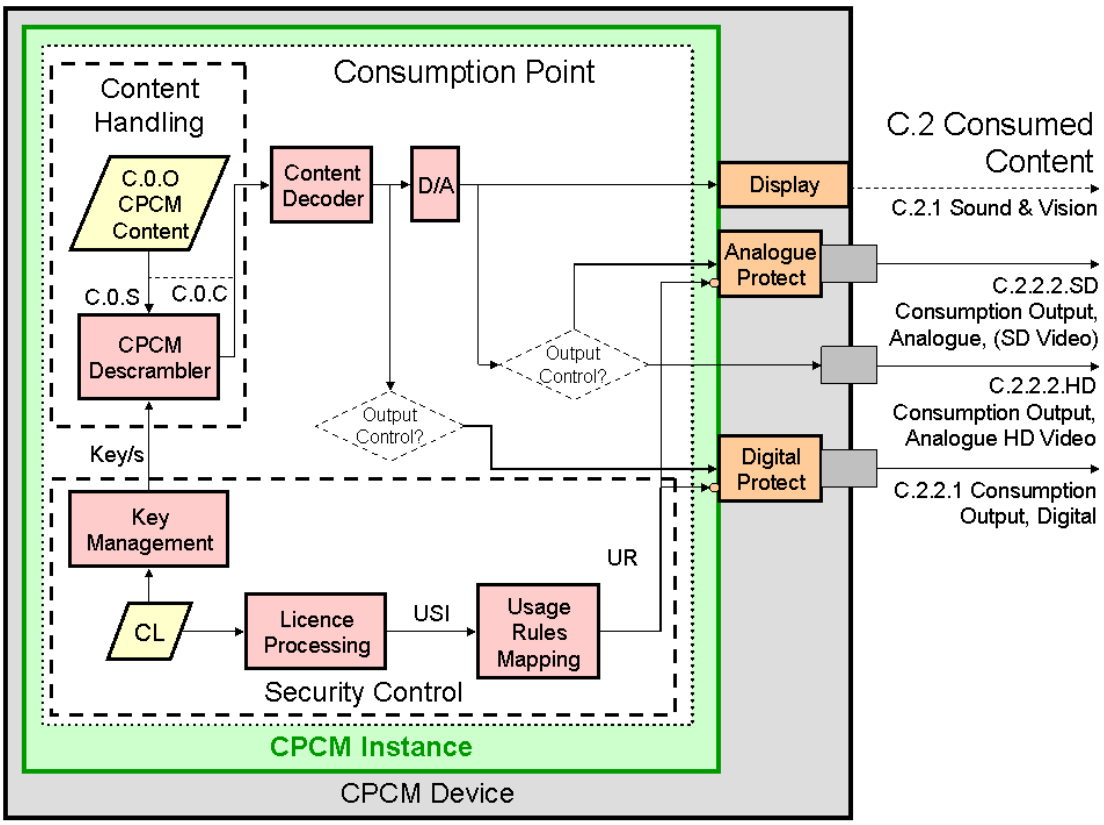

Figure 43: Consumption Point

The following clauses go into more detail about each type of Consumed Content.

11.6.2 Sound and Vision

C.2.1 Sound and Vision is Consumed Content that is directly rendered by the device hosting the Consumption Point.

11.6.3 Consumption Output

A Consumption Output (C.2.2) is an Output at a digital (C.2.2.1) or analogue (C.2.2.2) device interface, containing a transformation or signal that is intended to inhibit any other function than immediate consumption of that Content, i.e. to inhibit Storage of that Content. The method of transformation or signalling depends on the specific interface and is outside the scope of the Reference Model.

If necessary for any particular future Content type or format that is new to the consumer, it may be necessary to control C.2.2. Such control could constitute down-resolution of the image or even turning off the Consumption Output altogether. Such output control would be implemented as a CPCM Extension and shall only be activated for the future Content types or formats.

Such output control applied to CPCM Consumption Outputs is not foreseen in the baseline CPCM System because such a concept is alien to consumer expectations with current audio-video equipment, content types, delivery systems and business models, therefore such controls are reserved as optional features for the handling of new content types and usage models currently not available to consumers.

Depending on the type of CPCM Content concerned, a Consumption Output may be subject to the Output Control Usage Rule (clause 9.5), whereby the Consumption Point implementation needs to include the following controls on that Output:

- ability to enable and disable the output on C.2.2.2.SD Analogue Consumption Outputs for standard definition video for Content Items of the types necessitating this control;
- ability to enable and disable the output on C.2.2.2.HD Analogue Consumption Outputs for high definition video for Content Items of the types necessitating this control;

- ability to ensure that, if Image Constraint is signalled, a Content Item is passed through a Processing function that constrains the resolution of that Content Item prior to output of that Content Item on High Definition Analogue Consumption Outputs, the constraining function to be in accordance with the parameters specified in TS 102 825-3 [i.5].

11.7 Export

11.7.1 General

Exported Content is elaborated in order to differentiate between Trusted (C.3.1), Controlled (C.3.2) and Untrusted (C.3.3) Export, which are all digital. In addition there is Analogue Export (C.3.4).

Figure 44 shows this, building on the relevant part of the abstract model for Content classification.

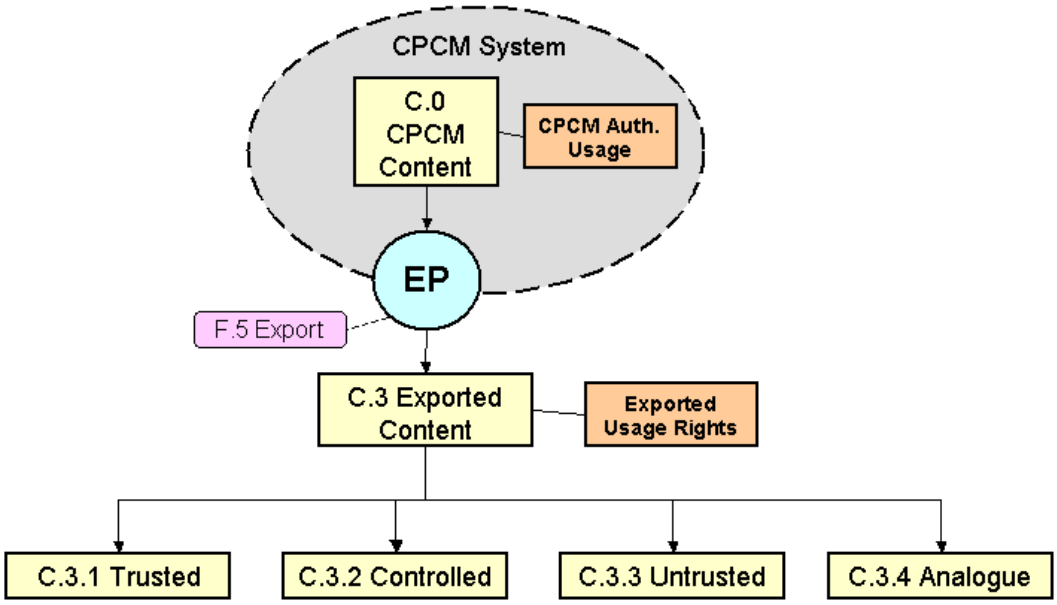

Figure 44: Exported Content

Figure 45 shows the logical model of the Export Point, based on the example of C.0.O.

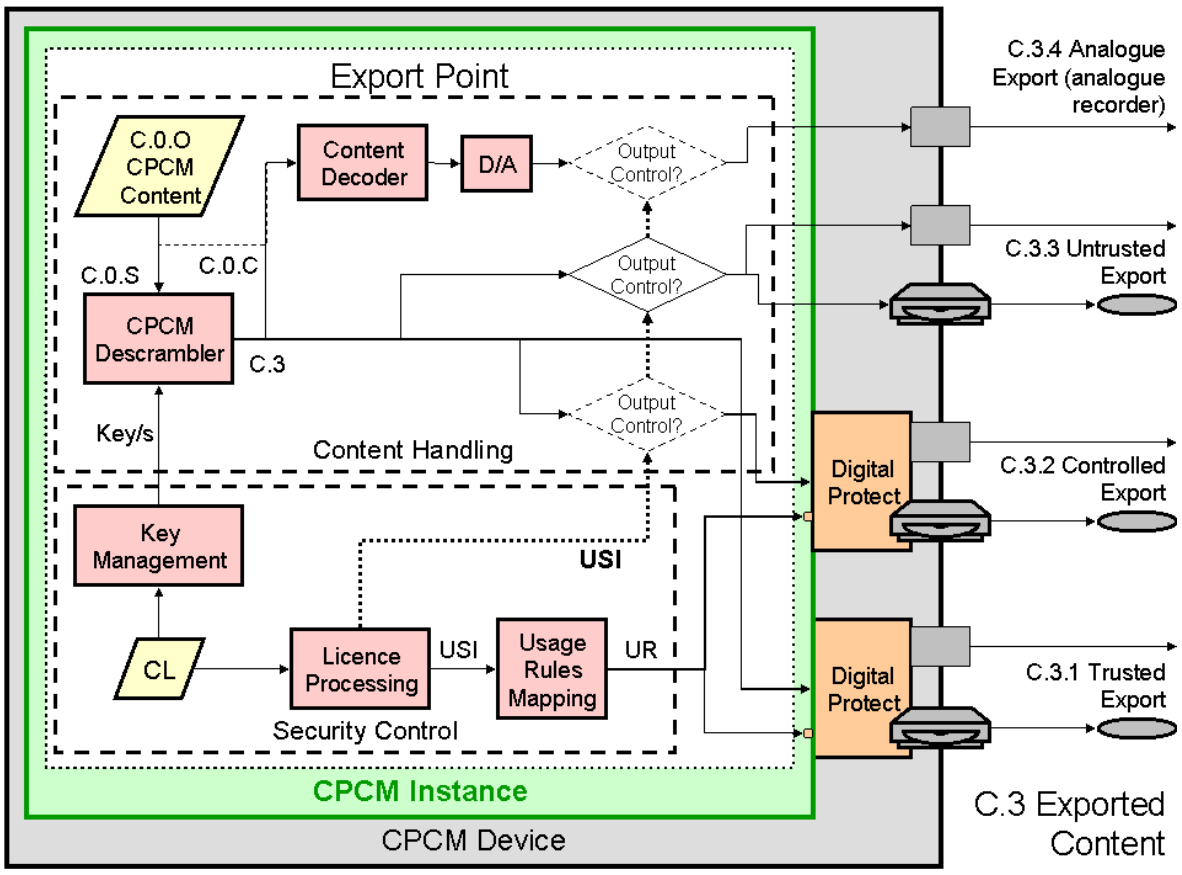

Figure 45: Export Point

Digital Exported Content, whether Trusted, Controlled or Untrusted, can be created in two basic ways - at a digital interface, or on a physical storage medium. Both constitute Outputs of CPCM Content. Analogue Exported Content can only be an Output at an analogue device interface.

The following clauses go into more detail about each type of Exported Content.

11.7.2 Trusted Export

Trusted Export (C.3.1) is a digital Output to a Trusted CPS for which there is a defined USI mapping, with no explicit control of the Output via USI for CPCM Content transferred to that Trusted CPS. The CPSs included under Trusted Export are defined by each C&R regime.

A CPS that is Trusted as an Output is not necessarily conversely Trusted as an Input (for Acquisition of content) to CPCM.

11.7.3 Controlled Export

Controlled Export (C.3.2) is the digital Output of CPCM Content mapped to a Trusted CPS under the explicit control of the Output Control Usage Rule (clause 9.5) assertion carried with that CPCM Content. The Trusted CPSs included under Controlled Export will be defined by an appropriate registration authority.

Controlled Export is a special case of Trusted Export, just as a Controlled CPS is a special case of a Trusted CPS.

11.7.4 Untrusted Export

Untrusted Export (C.3.3) is any digital output or storage format that is not Trusted (or Controlled). Untrusted Exported Content is not protected. The Exported Content may however still carry CPCM USI, if the Export format is compatible with the carriage of CPCM USI. Untrusted Export is under the explicit control of the Output Control Usage Rule (clause 9.5), in that Content can be exported to Untrusted Space only if its USI explicitly allow this.

11.7.5 Analogue Export

Analogue Exported Content (C.3.4) is an unprotected analogue Output, for example for the purpose of analogue recording.

Depending on the type of CPCM Content concerned, Analogue Export may be subject to the Output Control Usage Rule (clause 9.5).

Such Output control would be implemented as a CPCM Extension and shall only be activated for the future Content types or formats.

Analogue Export is also naturally subject to the Copy Control Usage Rule (clause 9.2), whereby CPCM Content carrying the copy control states CN or CNM shall not become Analogue Exported Content.

12 Extensions to CPCM

The clauses described so far define the CPCM baseline System. The CPCM baseline functionality may be extended where necessary, either for future additional extended CPCM functionality (CPCM Extension), or for particular proprietary functionality (proprietary Extension).

The protection and management of CPCM Content in the baseline CPCM System shall not be subverted by a CPCM Extension in any way.

CPCM will provide a common method for both types of Extension to interact with the CPCM Instance. Figure 46 shows how both types of Extension relate to the CPCM Instance and CPCM Device. The method of interaction is referred to as the CPCM Extension Interface, although it is unlikely to resemble any kind of physical or software interface, but rather take the form of rules and conditions about controls and data flows that are permitted to/from the CPCM Instance.

Whatever functionality they implement, both types of Extension are still subject to C&R regimes as for Trust Establishment with a CPCM Instance.

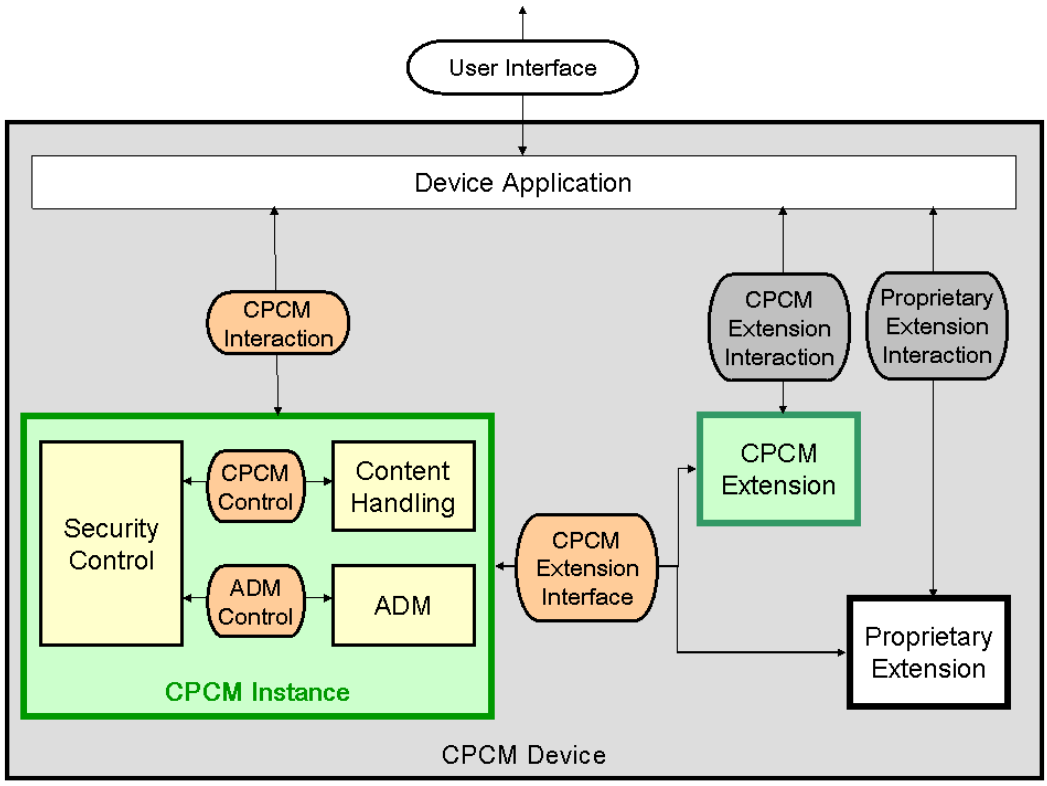

Figure 46: CPCM Device and CPCM Instance with Extensions

13 CPCM as an Interoperability Platform

The following elements of the CPCM System, previously described in terms of the CPCM Reference Model, provide the anchors for interoperability in the area of commercial content protection and management in the consumer environment.

The first of these are the CPCM security tools:

- CPCM Instance Certificate (CIC) format.
- Authenticated Key Exchange (AKE) mechanism - method of Trust Establishment and SAC management.
- Content cipher and mode of operation.

The set of CPCM Usage Rules and their corresponding coding in USI provide a common basis for many content provision and usage scenarios, able to accommodate content exchange to and from other systems via Usage Rules mappings.

Authorized Domain Management (ADM) provides the protocol and methods for CPCM Devices to manage their AD membership, if applicable.

The facilities of Content Acquisition into, and Content Export out of CPCM provide interoperability between CPCM and other Content Protection Systems (CPSs).

Naturally CPCM has a lot to do with home networking, but does not prescribe any particular requirements from its protocols or physical interfaces. CPCM is meant to work in a way that is transparent to the "home network", by being implemented as a secure resource controlled by the device's application on each compliant device, and by using the basic resources of the home network to carry out the necessary CPCM Communications between CPCM Devices as appropriate for those Devices.

List of figures

Figure 1: Scope of CPCM 9
Figure 2: CPCM System Conceptual Diagram 10
Figure 3: CPCM Functional Entities 11
Figure 4: CPCM Device Basic Model 12
Figure 5: Abstract Model - CPCM Functional Entities and Content Types with Nominal Notation 14
Figure 6: Abstract Model - Intra-CPCM Content types with Nominal Notation 15
Figure 7: Logical Model - CPCM Device 16
Figure 8: CPCM Instance Detail 19
Figure 9: CPCM Instance with Detail on Security Control 20
Figure 10: CPCM Instance with Detail on Content Handling 24
Figure 11: Logical Model - CPCM Instance and A.P.E.C.S. 25
Figure 12 CPCM Instance with Detail on Authorized Domain Management 26
Figure 13: CPCM Device Interfaces 28
Figure 14: CPCM Device and Physical Storage 29
Figure 15: CPCM Device Outputs and Non-CPCM Content 30
Figure 16: A Typical Authorized Domain 31
Figure 17: Logical Representation of Propagation Control Realms 35
Figure 18: The Local Environment in relation to two ADs 36
Figure 19: Localized ADs within an Authorized Domain 37
Figure 20: Notional Structure and Contents of the CPCM Content Licence 40
Figure 21: Depiction of CPCM Content with out-of-band (separate) CL 42
Figure 22: Depiction of CPCM Content with in-band (embedded) CL 42
Figure 23: Generic model of C.0.O Storage, and CL transfer protected by SAC 43
Figure 24: Basic Content Management Model 45
Figure 25: Input Content 46
Figure 26: Generic Logical Model of the Acquisition Point and Content Acquisition 47
Figure 27: Integrated-CA Acquisition 48
Figure 28: Smart-Card Based Acquisition Example 1 49
Figure 29: Smart-Card Based Acquisition Example 2 50
Figure 30: CA Module Based Acquisition Example 50
Figure 31: Acquisition of Free-To-View Example 1 51
Figure 32: Acquisition of Free-To-View Example 2 52
Figure 33: Acquisition from DRM System, Example 1 52

Figure 34: Acquisition from DRM System, Example 2 53
Figure 35: Acquisition from DRM System, Example 3 53
Figure 36: Acquisition of CPCM Clear Content Example 54
Figure 37: Acquisition from Trusted CPS 55
Figure 38: Stored and Retrieved Content 56
Figure 39: Storage Entity, Device interfaces and storage drives 57
Figure 40: Processing 58
Figure 41: Processing Entity 58
Figure 42: Consumed Content 59
Figure 43: Consumption Point 60
Figure 44: Exported Content 61
Figure 45: Export Point 62
Figure 46: CPCM Device and CPCM Instance with Extensions 63

History

Document history		
V1.1.1	July 2008	Publication