



Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 4: CPCM System Specification

EBU
OPERATING EUROVISION

DVB[®]
Digital Video
Broadcasting

ReferenceRTS/JTC-DVB-334-4

Keywordsbroadcast, digital, DVB, TV

ETSI

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

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

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

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

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

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

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

© European Telecommunications Standards Institute 2013.

© European Broadcasting Union 2013.

All rights reserved.

DECTTM, PLUGTESTSTM, UMTSTM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPPTM and LTETM are Trade Marks of ETSI registered for the benefit of its Members and
of the 3GPP Organizational Partners.
GSM[®] and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	10
Foreword.....	10
Introduction	10
1 Scope	11
2 References	11
2.1 Normative references	11
2.2 Informative references	12
3 Definitions and abbreviations.....	12
3.1 Definitions	12
3.2 Abbreviations	12
4 The CPCM System.....	12
4.1 General	12
4.2 CPCM Security toolbox	13
4.3 CPCM Authorized Domain Management	14
4.4 CPCM System versioning	14
4.5 CPCM Device physical interfaces.....	15
4.6 CPCM Instance Logical Interfaces.....	16
5 CPCM Data Types	19
5.1 General	19
5.2 Basic types.....	20
5.2.1 CPCM witness	20
5.2.2 CPCM trust check.....	20
5.2.3 CPCM Message Authentication Code (MAC).....	20
5.2.4 CPCM AD secret	20
5.2.5 Signed CPCM Instance Certificate	20
5.2.6 CPCM playback period.....	20
5.3 CPCM identifiers.....	20
5.3.1 CPCM Instance identifier	20
5.3.2 CPCM Certificate identifier.....	20
5.3.3 CPCM Authorized Domain Identifier.....	20
5.3.4 CPCM Content Licence Identifier	21
5.4 CPCM data structures.....	21
5.4.1 CPCM date and time	21
5.4.2 CPCM Instance Certificate Body.....	22
5.4.3 CPCM Instance Certificate chain.....	23
5.4.4 CPCM Content Licence	24
5.4.4.1 General	24
5.4.4.2 CPCM Descrambler information	25
5.4.4.3 CPCM Usage State Information.....	25
5.4.5 CPCM delivery signalling	28
5.4.6 CPCM status information	29
5.4.7 CPCM Content handling operation.....	30
5.4.8 CPCM Revocation List	31
5.4.9 CPCM Auxiliary Data	32
5.4.10 CPCM geographic location information	33
5.4.11 CPCM geographic location formats list.....	34
5.4.12 CPCM geographic area format	34
5.4.13 Other CPS Export data.....	35
5.4.14 CPCM rights issuer URL	35
5.4.15 CLC private data.....	36
5.4.16 Revocation List locator	36
5.4.17 AD name.....	37
5.4.18 AD capability.....	37

5.4.19	ADSE values.....	38
5.4.20	DC ADSE value list.....	38
5.4.21	DC Local identifiers list.....	39
5.4.22	AD internal record	39
5.4.23	AD internal record list	40
5.4.24	CPCM extension data element.....	40
5.4.25	Private element structure	40
5.4.26	Key Recovery Information structure.....	41
5.4.27	External scrambling information structure (optional).....	41
6	CPCM protocols.....	43
6.1	General	43
6.2	CPCM protocol message framework.....	43
6.2.1	General.....	43
6.2.2	CPCM protocol message	45
6.2.2.1	General	45
6.2.2.2	Conditional elements.....	46
6.2.2.3	Optional elements	46
6.2.2.4	Element identifiers	47
6.2.2.5	CPCM protocol message type	48
6.2.2.6	Control field	49
6.2.3	Generic atomic transaction	50
6.2.4	CPCM protocol timeouts	54
6.2.5	CPCM protocol bridging	55
6.3	General CPCM protocol messages	55
6.3.1	General.....	55
6.3.2	CPCM protocol error	55
6.3.2.1	General	55
6.3.2.2	CPCM protocol generic error codes	56
6.3.3	CPCM protocol transaction rollback	57
6.4	CPCM security control protocols.....	58
6.4.1	General.....	58
6.4.2	SAC establishment.....	59
6.4.2.1	General	59
6.4.2.2	CPCM AKE initiation.....	60
6.4.2.3	CPCM AKE commit	61
6.4.2.4	CPCM AKE renew.....	62
6.4.2.5	CPCM AKE commit renew	63
6.4.2.6	CPCM AKE confirm.....	63
6.4.2.7	CPCM AKE confirm response	64
6.4.2.8	CPCM AKE terminate	64
6.4.3	CPCM AD Secret management	65
6.4.3.1	General	65
6.4.3.2	Deliver AD Secret	65
6.4.3.3	Deliver AD Secret response	66
6.4.3.4	Erase AD Secret	67
6.4.3.5	Erase AD Secret response	67
6.5	CPCM System and Content Management Protocols	68
6.5.1	General.....	68
6.5.2	CPCM instance status	70
6.5.2.1	General	70
6.5.2.2	CPCM Instance status enquiry	71
6.5.2.3	CPCM Instance status enquiry response	71
6.5.3	CPCM Content Licence exchange	72
6.5.3.1	General	72
6.5.3.2	CPCM get Content Licence	73
6.5.3.3	CPCM get Content Licence response.....	74
6.5.3.4	CPCM get new Content Licence	75
6.5.3.5	CPCM put Content Licence	76
6.5.3.6	CPCM put Content Licence response	76
6.5.4	CPCM Content operation permission	77
6.5.4.1	General	77

6.5.4.2	CPCM get permission	78
6.5.4.3	CPCM get permission response	78
6.5.5	CPCM Content item status protocol	79
6.5.5.1	General	79
6.5.5.2	CPCM get Content item status request	79
6.5.5.3	CPCM get Content item status response	80
6.5.6	CPCM Device Proximity Checks	81
6.5.6.1	General	81
6.5.6.2	Proximity method description	81
6.5.6.3	Proximity Tools	82
6.5.6.3.1	Round Trip Time protocol (RTT)	82
6.5.6.3.2	Secured Round Trip Time protocol (SRTT)	83
6.5.6.3.3	Re-using GPS or Terrestrial Triangulation for Proximity (GTTP)	86
6.5.6.3.4	Proximity Through Association (PTA)	87
6.5.6.3.5	Proximity Assignment by Authorized Authenticated Agent (PAAAA)	89
6.5.6.3.6	Proximity through direct connection (PTDC)	91
6.5.6.4	Mandatory Proximity tools	91
6.5.7	CPCM secure time	91
6.5.7.1	General	91
6.5.7.2	CPCM get absolute time	92
6.5.7.3	CPCM get absolute time response	92
6.5.8	Geographic information	93
6.5.8.1	General	93
6.5.8.2	CPCM enquire geographic location formats	94
6.5.8.3	CPCM geographic location formats response	94
6.5.8.4	CPCM get geographic location	95
6.5.8.5	CPCM get geographic location response	96
6.5.8.6	CPCM affirm geographic location	96
6.5.8.7	CPCM affirm geographic location response	97
6.5.9	AD membership challenge	97
6.5.9.1	General	97
6.5.9.2	CPCM AD membership challenge	98
6.5.9.3	CPCM AD membership challenge response	99
6.5.10	CPCM Content Licence Move	99
6.5.10.1	General	99
6.5.10.2	CPCM Content Licence Move begin	101
6.5.10.3	CPCM Content Licence Move ready	102
6.5.10.4	CPCM Content Licence Move commit	102
6.5.10.5	CPCM Content Licence Move confirm	103
6.5.10.6	CPCM Content Licence Move finish	104
6.5.10.7	CPCM Content Licence Move request	104
6.5.10.8	CPCM Content Licence Move response	105
6.5.11	CPCM Discovery	106
6.5.11.1	General	106
6.5.11.2	Discovery request	106
6.5.11.3	Discovery response	107
6.5.12	CPCM Revocation List Acquisition	108
6.5.12.1	General	108
6.5.12.2	Get CPCM Revocation List	108
6.5.12.3	Notify CPCM Revocation List	109
6.5.13	CPCM Content Discovery	109
6.5.13.1	General	109
6.5.13.2	Content Discovery request	110
6.5.13.3	Content Discovery response	110
6.6	Authorized Domain management protocols	111
6.6.1	General	111
6.6.2	ADM Enumerated Fields	115
6.6.2.1	General	115
6.6.2.2	ADM status	115
6.6.2.3	ADM condition	115
6.6.2.4	ADM protocol	115
6.6.2.5	Delegating CPCM Instance identifier	115

6.6.2.6	Local Master capability.....	116
6.6.2.7	CPCM version.....	116
6.6.2.8	Remotely Joined CICFs list	116
6.6.3	General ADM protocols.....	116
6.6.3.1	General	116
6.6.3.2	AD update request.....	116
6.6.3.3	AD update response	117
6.6.3.4	AD update indication	118
6.6.3.5	AD change request	119
6.6.3.6	AD change response.....	119
6.6.3.7	ADM quorum test query	120
6.6.3.8	ADM quorum test response	121
6.6.3.9	ADM invite	122
6.6.3.10	ADM invite result	123
6.6.4	AD Join.....	124
6.6.4.1	General	124
6.6.4.2	AD Join begin	124
6.6.4.3	AD Join ready	125
6.6.4.4	AD Join commit	126
6.6.4.5	AD Join confirm.....	126
6.6.4.6	AD Join finish	127
6.6.5	AD Leave.....	128
6.6.5.1	General	128
6.6.5.2	AD Leave begin	128
6.6.5.3	AD Leave ready	129
6.6.5.4	AD Leave commit	130
6.6.5.5	AD Leave confirm.....	131
6.6.5.6	AD Leave finish	131
6.6.6	Local Master election.....	132
6.6.6.1	General	132
6.6.6.2	Local Master election request	132
6.6.6.3	Local Master election response	133
6.6.6.4	Local Master election indication	134
6.6.7	Domain Controller transfer	135
6.6.7.1	General	135
6.6.7.2	Domain Controller transfer begin	135
6.6.7.3	Domain Controller transfer ready	136
6.6.7.4	Domain Controller transfer commit	137
6.6.7.5	Domain Controller transfer confirm.....	137
6.6.7.6	Domain Controller transfer finish	138
6.6.7.7	Become Domain Controller	139
6.6.7.8	New Domain Controller	139
6.6.8	Domain Controller split	140
6.6.8.1	General	140
6.6.8.2	Domain Controller split begin.....	140
6.6.8.3	Domain Controller Split ready	141
6.6.8.4	Domain Controller split commit	142
6.6.8.5	Domain Controller split confirm	143
6.6.8.6	Domain Controller split finish.....	144
6.6.9	Domain Controller Merge.....	144
6.6.9.1	General	144
6.6.9.2	Domain Controller merge begin.....	144
6.6.9.3	Domain Controller merge ready.....	145
6.6.9.4	Domain Controller Merge commit.....	146
6.6.9.5	Domain Controller merge confirm.....	147
6.6.9.6	Domain Controller merge finish	147
6.6.9.7	Merge Domain Controller	148
6.6.9.8	Domain Controller Merged	148
6.6.10	Domain Controller rebalance.....	149
6.6.10.1	General	149
6.6.10.2	Domain Controller rebalance begin	149
6.6.10.3	Domain Controller rebalance ready	150

6.6.10.4	Domain Controller rebalance commit	151
6.6.10.5	Domain Controller rebalance confirm	151
6.6.10.6	Domain Controller rebalance finish	152
6.6.10.7	Rebalance Domain Controller	152
6.6.10.8	Domain Controller rebalanced	153
6.6.11	ADMAAA management	154
6.6.11.1	General	154
6.6.11.2	ADMAAA tool request	154
6.6.11.3	ADMAAA tool response	155
6.7	CPCM Extension messages	155
6.8	Private message	156
7	CPCM Content Management	157
7.1	General	157
7.2	CPCM Device and Content discovery	158
7.3	Inter-Device CPCM Content exchange	160
7.4	CPCM functional entity behaviour	161
7.4.1	Acquisition	161
7.4.2	Processing	162
7.4.3	Export	162
7.4.4	Consumption	163
7.4.5	Storage	163
7.5	USI enforcement	164
7.5.1	General	164
7.5.2	Controls prior to Content transfer	164
7.5.2.1	Copy and Movement control	164
7.5.2.1.1	Copy Control Not Asserted	164
7.5.2.1.2	Copy Once	164
7.5.2.1.3	Copy No More	164
7.5.2.1.4	Copy Never and Zero Retention	164
7.5.2.2	Consumption Control	164
7.5.2.2.1	Viewable	164
7.5.2.2.2	View Window Activated	165
7.5.2.2.3	View Period Activated	165
7.5.2.2.4	Simultaneous View Count Activated	165
7.5.2.3	Propagation Control	166
7.5.2.3.1	MLAD and VLAD	167
7.5.2.3.2	MGAD and VGAD	167
7.5.2.3.3	MAD and VAD	167
7.5.2.3.4	MCPCM and VCPCM	168
7.5.2.3.5	MLocal and VLocal	168
7.5.2.4	Export/Output Control	168
7.5.2.5	Ancillary Control	168
7.5.3	Controls to be enforced when receiving Content	168
7.5.3.1	Copy and Movement Control	168
7.5.3.1.1	Copy Control Not Asserted	168
7.5.3.1.2	Copy Once	169
7.5.3.1.3	Copy No More	169
7.5.3.1.4	Copy Never and Zero Retention	169
7.5.3.2	Consumption control	169
7.5.3.2.1	Viewable	169
7.5.3.2.2	View Window Activated	169
7.5.3.2.3	View Period Activated	169
7.5.3.2.4	Simultaneous View Count Activated	169
7.5.3.3	Propagation control	170
7.5.3.3.1	MLAD and VLAD	170
7.5.3.3.2	MGAD and VGAD	170
7.5.3.3.3	MAD and VAD	171
7.5.3.3.4	MCPCM and VCPCM	171
7.5.3.3.5	MLocal and VLocal	171
7.5.3.4	Export and Consumption output control	171
7.5.3.5	Ancillary control	172

7.5.4	Remote Access rules	172
7.5.4.1	General	172
7.5.4.2	Remote Access post record	172
7.5.4.3	Remote Access post date/time (moving window)	173
7.5.4.4	Remote Access post date/time (immediate)	173
7.6	CPCM Content Scrambling management	173
7.6.1	General	173
7.6.2	Dynamic changes of the CPCM Content scrambling key	173
7.7	Content Move operation	174
7.7.1	Introduction	174
7.7.2	Source CPCM Instance behaviour with Content Move	175
7.7.2.1	Content Handling Behaviour	175
7.7.2.2	Security control behaviour	178
7.7.3	Sink CPCM Instance behaviour with Content Move	178
7.7.3.1	Content handling behaviour	178
7.7.3.2	Security control behaviour	180
7.7.4	Abnormal behaviour	180
7.7.5	Failure recovery	180
7.8	CPCM Content Revocation	181
7.8.1	General	181
7.8.2	CPCM Instance-based Content revocation	182
7.8.3	AD based Content revocation	182
7.9	CPCM Content interoperability between C&R regimes	183
8	CPCM Content Licence management	183
8.1	General	183
8.2	CPCM Content Licence generation	184
8.2.1	CL generation upon Content Acquisition	184
8.2.1.1	General	184
8.2.1.2	CPCM version	184
8.2.1.3	Content Licence protection	184
8.2.1.4	Descrambler information	184
8.2.1.5	Content Licence identifier	184
8.2.1.6	Content Licence creator	185
8.2.1.7	Last CL issuer	185
8.2.1.8	C&R regime mask	185
8.2.1.9	RL index list	185
8.2.1.10	Authorized Domain identifier	185
8.2.1.11	Descrambling key	185
8.2.1.12	Usage State Information	186
8.2.1.13	CPCM Auxiliary Data digest	186
8.2.1.14	AD Secret Signature	186
8.2.1.15	CPCM Auxiliary Data	186
8.2.2	CL generation in other cases	186
8.2.2.1	General	186
8.2.2.2	Content Licence protection	187
8.2.2.3	Descrambler information	187
8.2.2.4	Content Licence identifier	187
8.2.2.5	Last CL issuer	187
8.2.2.6	Authorized Domain identifier	187
8.2.2.7	Descrambling key	187
8.2.2.8	Usage State Information	187
8.2.2.9	CPCM Auxiliary Data digest	188
8.2.2.10	AD Secret Signature	188
8.2.2.11	CPCM Auxiliary Data	188
8.3	CPCM Content Licence identification	188
8.3.1	General	188
8.3.2	CIC Identifier (only)	189
8.3.3	ISAN	190
8.3.4	Truncated ISAN	190
8.4	CPCM Content Licence verification	191
8.5	Content Licence re-Acquisition	191

8.6	Content Licence protection.....	192
8.6.1	CL protection modes.....	192
8.6.2	CL protection mode usage	193
8.6.3	CL protection mode changes	194
History		205

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Full standard:
<https://standards.iteh.ai/catalog/standards/sist/70fb22e-c41d-439d-96b3-3bc04c7b3cb9/etsi-ts-102-825-4-v1.2.2-2013-12>

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://ipr.etsi.org>).

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 SACCONNEX (Geneva)
Switzerland
Tel: +41 22 717 21 11
Fax: +41 22 717 24 81

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

The present document is part 4 of a multi-part deliverable. Full details of the entire series can be found in part 1 [6].

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 is the specification of the Digital Video Broadcasting (DVB) Content Protection and Copy Management (CPCM) System. It contains the generic specification applicable to all deployments of CPCM. Technology-specific adaptations for content formats, storage formats, home network ecosystems and application-specific physical interfaces are contained in TS 102 825-9 [5].

2 References

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

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

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

2.1 Normative references

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

- [1] ETSI EN 300 468: "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems".
 - [2] IEEE List of Registered OUI.
- NOTE: Available at <http://standards.ieee.org/regauth/oui/index.shtml>.
- [3] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions - Part 1: Country codes".
 - [4] ETSI TS 101 162: "Digital Video Broadcasting (DVB); Allocation of identifiers and codes for Digital Video Broadcasting (DVB) systems".
 - [5] ETSI TS 102 825-9: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 9: CPCM System Adaptation Layers".
 - [6] ETSI TS 102 825-1: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 1: CPCM Abbreviations, Definitions and Terms".
 - [7] ETSI TS 102 825-5: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 5: CPCM Security Toolbox".
 - [8] ETSI TS 102 825-7: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 7: CPCM Authorized Domain Management".
 - [9] ETSI TS 102 825-10: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 10: CPCM Acquisition, Consumption and Export Mappings".
 - [10] ETSI TS 102 825-3: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 3: CPCM Usage State Information".

2.2 Informative references

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

- [i.1] ETSI TS 101 154: "Digital Video Broadcasting (DVB); Specification for the use of Video and Audio Coding in Broadcasting Applications based on the MPEG-2 Transport Stream".
- [i.2] ETSI TS 102 005: "Digital Video Broadcasting (DVB); Specification for the use of Video and Audio Coding in DVB services delivered directly over IP protocols".
- [i.3] ETSI TS 102 825-2: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 2: CPCM Reference Model".
- [i.4] ETSI TR 102 825-8: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 8: CPCM Authorized Domain Management scenarios".
- [i.5] ETSI TR 102 825-11: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 11: CPCM Content management scenarios".
- [i.6] ETSI TR 102 825-12: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 12: CPCM Implementation Guidelines".
- [i.7] ETSI TS 102 825-14: "Digital Video Broadcasting (DVB); Content Protection and Copy Management (DVB-CPCM); Part 14: CPCM Extensions".
- [i.8] ETSI TR 101 289: "Digital Video Broadcasting (DVB); Support for use of scrambling and Conditional Access (CA) within digital broadcasting systems".
- [i.9] ARIB STD25: "Conditional Access System specifications for digital broadcasting".
- [i.10] DVB Bluebook A125: "Support for use of the DVB scrambling algorithm version 3 within digital broadcasting system".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 102 825-1 [6] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TS 102 825-1 [6] apply.

4 The CPCM System

4.1 General

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 CPCM Reference Model (TS 102 825-2 [i.3]) and the CPCM Abbreviations, Definitions and Terms (TS 102 825-1 [6]) provide the foundation upon which this CPCM System specification is based. The CPCM System specification populates each of the aspects of the CPCM Reference Model in order to define a complete and implementable system.

The main body of the present document provides the generic specification of the CPCM System, applicable to all deployments of CPCM.

The generic CPCM System specification defines the aspects of the CPCM System that apply to all deployments of CPCM. The remaining of this clause deal with the following elements of the CPCM System:

- CPCM Security Toolbox;
- CPCM Authorized Domain Management (ADM);
- CPCM System versioning;
- CPCM Device physical interfaces; and
- CPCM Instance logical interfaces.

The subsequent clauses of the CPCM System generic specification, starting in clause 5, deal with the following elements:

- **CPCM data formats:** the generic CPCM System specification contains a common set of CPCM-specific data type definitions used by every CPCM System deployment. The CPCM Data Types are documented in clause 5.
- **CPCM protocols:** the generic CPCM System specification defines a set of protocols that are used by all CPCM Instances in order to enable CPCM Content exchanges and exchange CPCM-relevant data. The CPCM protocols are specified in clause 6.
- **CPCM Content management:** individual aspects of CPCM System behaviour relating to the handling of CPCM Content are specified in clause 7.
- **CPCM Content Licence management:** clause 8 deals with all aspects around the generation and handling of CPCM Content Licences.

Various end-to-end CPCM Content handling scenarios, as well as ADM scenarios, are documented in TR 102 825-8 [i.4] and TR 102 825-11 [i.5], building on the individual content handling aspects from clauses 7 and 8.

The CPCM System is designed to provide a generic content protection and management platform that can be adapted to various content ecosystems. A content ecosystem can consist of one or more aspects to which the CPCM System Specification is adapted in order to provide a complete and workable content protection and management solution. These aspects of adaptation are:

- **Content format:** a CPCM System deployment needs at least one content format adaptation. CPCM System content format adaptations are defined in TS 102 825-9 [5].
- **Storage format:** if a CPCM System deployment includes the ability to Store CPCM Content then it needs at least one storage format. CPCM System storage format adaptations are defined in TS 102 825-9 [5].
- **Home Network ecosystem:** a home network ecosystem adaptation is needed for the CPCM System to work within that ecosystem. Specifications of CPCM System adaptations for particular home network ecosystems are contained in TS 102 825-9 [5].
- **Application-specific physical interface:** the CPCM System can be adapted to provide content protection and management functionality over an application-specific physical interface that benefits from re-using the CPCM tools and facilities. TS 102 825-9 [5] contains the definitions for CPCM System adaptations for particular application-specific physical interfaces.

4.2 CPCM Security toolbox

The CPCM Security Toolbox is the set of cryptographic algorithms and methods that enables the protection of CPCM Content, as required by the provider of that content, throughout its lifetime within the CPCM System.

The set of CPCM security tools in the toolbox do not provide any alternative methods for performing any particular security-related task within the CPCM System. Rather, there is one tool specified for each security-related task.