



INTERNATIONAL STANDARD

NORME INTERNATIONALE



Internet protocol (IP) and transport stream (TS) based service access

Accès aux services fondé sur le protocole internet (IP) et sur le flux de transport (TS)

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 33.170; 35.100.05; 35.240.99

ISBN 978-2-8322-1048-2

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

FOREWORD.....	14
1 Scope.....	16
2 Normative references	16
3 Terms, definitions and abbreviations	18
3.1 Terms and definitions	18
3.2 Symbols	23
3.3 Abbreviations	24
3.4 Identifiers assigned by external entities.....	28
4 General	28
4.1 Overview	28
4.2 General description of the system and elements.....	29
4.2.1 General	29
4.2.2 Selected technologies	30
4.2.3 Overview of four-layer model for service protection	31
4.3 End-to-end system	33
4.4 Supported systems and device types.....	33
4.5 Service protection versus content protection	35
5 General specifications	36
5.1 End-to-end architecture	36
5.2 Special cases	38
5.2.1 Free-to-air services	38
5.2.2 Free-to-view services	38
5.3 Service guide and purchase	38
5.4 Four-layer model – Key hierarchy.....	39
5.4.1 General	39
5.4.2 Keys on the traffic layer.....	40
5.4.3 Keys on the key stream layer.....	40
5.4.4 Keys on the rights management layer (interactive mode)	43
5.4.5 Keys on the rights management layer (broadcast mode).....	43
5.4.6 Keys on the registration layer (interactive mode)	43
5.4.7 Keys on the registration layer (broadcast mode).....	43
5.4.8 Authentication overview.....	46
5.5 Deployment for broadcast mode of operation.....	47
5.5.1 Concept of Domains –Interactive and broadcast domains	47
5.5.2 Addressing (group/subset/device/domain)	48
5.5.3 Zero message broadcast encryption scheme	51
6 Traffic layer.....	53
6.1 General	53
6.2 IPsec.....	53
6.2.1 General	53
6.2.2 Selectors	54
6.2.3 Encapsulation protocol and mode	54
6.2.4 Encryption algorithm.....	55
6.2.5 Authentication algorithm	55
6.2.6 Security association management	55
6.3 ISMACryp.....	55

6.3.1	Streamed content	55
6.3.2	Downloadable audio/visual content (stored in MP4 files).....	56
6.3.3	Use of ISMACryp with the rights management and key stream layers	57
6.4	SRTP	57
6.4.1	General	57
6.4.2	Key management.....	59
6.4.3	Encryption algorithm.....	60
6.4.4	Authentication algorithm	60
6.5	MPEG2 TS crypt	60
6.5.1	General	60
6.5.2	Transport stream level scrambling	62
6.5.3	PES level scrambling.....	62
6.5.4	Descrambling MPEG2 content	63
6.5.5	Supported ciphers	64
6.5.6	Key management.....	64
7	Key stream layer	65
7.1	General.....	65
7.2	Format of the key stream message (KSM).....	65
7.2.1	Format.....	65
7.2.2	Descriptors for access_criteria_descriptor_loop.....	68
7.2.3	Constants	75
7.2.4	Coding and semantics of attributes.....	75
8	Rights management layer	83
8.1	General	83
8.2	Identification of rights objects	83
8.3	Requirements for rights objects	84
8.3.1	Requirements for service ROs	84
8.3.2	Requirements for programme ROs.....	84
8.4	Format of rights objects.....	85
8.4.1	Format of an Interactivity channel rights object (ICRO).....	85
8.4.2	Format of a broadcast rights object (BCRO)	85
8.4.3	Format of the asset object	89
8.4.4	Format of the permission object.....	92
8.4.5	Format of the action object	93
8.4.6	Format of the constraint object	94
9	Registration layer	100
9.1	General	100
9.2	RI context.....	100
9.3	Registration layer protocols and message specification	101
9.3.1	Interactivity channel registration layer specification	101
9.3.2	Broadcast channel registration layer specification	101
9.3.3	Domain joining and leaving.....	136
9.3.4	Token handling	151
9.3.5	Mixed-mode registration for interactive and broadcast modes of operation	158
10	Signalling and service guide	159
10.1	General	159
10.2	Signalling requirements	160
10.2.1	Signalling information	160

10.2.2	Requirements for signalling the KSM	160
10.2.3	Requirements for signalling of services	160
10.3	Service guide requirements	160
10.4	Service guide recommendations	160
11	Rights issuer services and rights issuer streams	161
11.1	General	161
11.2	Rights issuer services	161
11.2.1	Requirements for rights issuer services in IPDC over DVB-H systems	161
11.2.2	Requirements for rights issuer services in DVB-T/C/S systems	162
11.2.3	Requirements for the support of rights issuer services and streams in IPTV systems	162
11.3	Usage of rights issuer streams and services	162
11.3.1	General	162
11.3.2	Scheduled RI stream	163
11.3.3	<i>Ad hoc</i> RI stream	163
11.3.4	In-band RI streams within a media service	163
12	Service subscription and purchase	165
12.1	General	165
12.2	Purchase over an interactivity channel	166
12.2.1	General	166
12.2.2	Typical purchase sequences	167
12.2.3	Protocol	188
12.2.4	XML schemas for request and response messages	189
12.2.5	XML schema definition for request and response related XML elements	203
12.3	Purchase for mixed-mode devices	207
12.4	Out-of-band purchase	208
12.4.1	Means of purchase – Introduction	208
12.4.2	Out-of-band purchase from service guide data	208
12.5	Required service guide Information	210
12.5.1	General	210
12.5.2	Service operation centre (including service distribution management)	211
12.5.3	Customer operation centre (including service subscription management)	211
12.5.4	Service	212
12.5.5	ScheduleItem	213
12.5.6	ContentItem	213
12.5.7	Purchase item	214
12.5.8	Purchase data	214
13	Protection of IPDC over DVB-H systems	214
13.1	General	214
13.2	Delivery of traffic layer data in IPDC over DVB-H systems	215
13.3	Delivery of key stream data in IPDC over DVB-H systems	215
13.4	Delivery of rights management data in IPDC over DVB-H systems	215
13.4.1	General	215
13.4.2	Delivery of ICROs in IPDC over DVB-H systems over interactivity channel	215
13.4.3	Delivery of BCROs in IPDC over DVB-H systems over broadcast channel	215
13.5	Delivery of registration data in IPDC over DVB-H systems	215

13.5.1	General	215
13.5.2	Delivery of registration data in IPDC over DVB-H systems over an interactivity channel.....	216
13.5.3	Delivery of registration data in IPDC over DVB-H systems over a broadcast channel	216
13.6	Signalling and service guides in IPDC over DVB-H systems	216
13.6.1	General	216
13.6.2	Signalling of KSM in IPDC over DVB-H systems	216
13.6.3	The service guide for IPDC over DVB-H systems.....	217
13.7	Format and use of RI streams over IPDC over DVB-H systems	217
13.7.1	General	217
13.7.2	IP characteristics.....	218
13.7.3	RI stream packet format	218
13.7.4	Implementation notes	220
13.7.5	Mapping of messages to RI services and streams	221
13.7.6	Discovery of RI services, streams and schedule Information	221
13.7.7	Certificate chain updates.....	222
13.7.8	Resending of BCROs	222
13.7.9	Summary of requirements for rights issuers.....	223
13.7.10	Summary of requirements for devices.....	223
13.7.11	Mapping of messages to DVB-H time sliced bursts.....	224
14	Protection of DVB T/C/S systems	224
14.1	General	224
14.2	Delivery of traffic layer data in DVB T/C/S systems	225
14.3	Delivery of key stream data in DVB T/C/S systems	225
14.4	Delivery of rights management data in DVB T/C/S systems	226
14.4.1	General	226
14.4.2	Delivery of ICROs in DVB T/C/S systems over interactivity channel	226
14.4.3	Delivery of BCROs in DVB T/C/S systems over broadcast channel.....	226
14.5	Delivery of registration data in DVB T/C/S systems	227
14.5.1	General	227
14.5.2	Delivery of registration data in DVB T/C/S systems over an interactivity channel	227
14.5.3	Delivery of registration data in DVB T/C/S systems over a broadcast channel	227
14.5.4	Registration message table	228
14.6	Signalling and service guide in DVB T/C/S systems	230
14.6.1	General	230
14.6.2	Signalling of encrypted services in DVB T/C/S systems.....	231
14.6.3	SI tables	239
14.6.4	SI descriptors	248
14.7	User-defined identifiers used in DVB-SI tables	262
14.8	Scope of identifiers used in DVB-SI tables	262
14.9	Format of RI services over DVB-T/C/S systems.....	263
14.9.1	General	263
14.9.2	RI stream packet format	263
14.9.3	Addressing of objects	263
14.9.4	Mapping of messages to RI services and streams	263
15	Protection of MPEG2 TS-based IP systems	263
15.1	General.....	263

15.2	Encapsulation of an MPEG2 TS in IP	264
15.3	Delivery of traffic layer data in MPEG2 TS-based IP systems	264
15.4	Delivery of key stream data in MPEG2 TS-based IP systems	264
15.5	Delivery of rights management data in MPEG2 TS-based IP systems	264
15.6	Delivery of registration data in MPEG2 TS-based IP systems	264
15.7	Signalling and service guides in MPEG2 TS-based IP systems	264
15.7.1	General	264
15.7.2	Signalling and the service guide in DVB-IPI systems	264
15.7.3	Signalling and service guides in non-DVB-IPI systems	267
15.8	Format of RI services over MPEG2 TS-based IP systems	267
15.9	Content-on-demand support	267
15.9.1	General	267
15.9.2	Content-on-demand trick play support	268
15.10	Use of server-side purchase interfaces	268
15.10.1	General	268
15.10.2	Example showing registration via a web interface	269
15.10.3	Example showing purchase via a web interface	269
16	Protection of non-MPEG2 TS-based IP systems	269
16.1	General	269
16.2	Delivery of traffic layer data in non-MPEG2 TS-based IP systems	269
16.3	Delivery of key stream data in non-MPEG2 TS-based IP systems	270
16.4	Delivery of rights management data in non-MPEG2 TS-based IP systems	270
16.5	Delivery of registration data in non-MPEG2 TS-based IP systems	270
16.6	Signalling and service guides in non-MPEG2 TS-based IP systems	270
16.7	Format of RI services over non-MPEG2 TS-based IP systems	270
16.8	Content-on-demand support	270
Annex A (normative)	Supporting specifications	271
Annex B (informative)	Deployment considerations	354
Bibliography	406
Figure 1	– System overview	29
Figure 2	– Service protection via four-layer model	31
Figure 3	– Highly simplified view of the end-to-end system	33
Figure 4	– Service protection versus content protection	35
Figure 5	– Service protection and purchase entities and names (broadcast architecture)	36
Figure 6	– Public key infrastructure	37
Figure 7	– Overview of service guide and purchase	39
Figure 8	– 4-layer key hierarchy – Use of SEK only	41
Figure 9	– 4-layer key hierarchy – Use of PEK and SEK	42
Figure 10	– Authentication hierarchy	46
Figure 11	– Explaining the concept of addressing	48
Figure 12	– (Oversimplified) group BCRO	49
Figure 13	– (Oversimplified) subscriber group BCRO	49
Figure 14	– (Oversimplified) unique device BCRO	50
Figure 15	– (Oversimplified) broadcast domain BCRO	50
Figure 16	– Example of a zero message tree with three nodes (keys)	51

Figure 17 – IPsec security association elements	54
Figure 18 – ISMACryp Key Management.....	57
Figure 19 – SRTP cryptographic context management.....	59
Figure 20 – MPEG2 transport stream cryptographic context management.....	61
Figure 21 – Single-key versus dual-key TS over time.....	63
Figure 22 – Registration for broadcast mode of operation with one ROT	102
Figure 23 – Offline NDD protocol	103
Figure 24 – Samples of notification displays	104
Figure 25 – Off-line NSD protocol	104
Figure 26 – Action request code (ARC).....	104
Figure 27 – Samples of notification displays showing an ARC message.....	106
Figure 28 – Sample of token consumption reporting notification display.....	107
Figure 29 – Sample of TAA report display	108
Figure 30 – 1-pass PDR protocol – (first) device registration.....	109
Figure 31 – 1-pass IRD protocol – RI initiated message to device (here re-registration).....	109
Figure 32 – Unique device number	112
Figure 33 – Device_registration_response() message.....	122
Figure 34 – Structure of device_registration_response() message	123
Figure 35 – Domain_registration_response() message.....	142
Figure 36 – Structure of domain_registration_response() message	143
Figure 37 – Registration for mixed-mode operation with one ROT.....	159
Figure 38 – Relationship between RI service and RI streams and other services and RI Streams	163
Figure 39 – Message flows for service subscription and purchase for the connected mode of operation.....	165
Figure 40 – Message flows for service subscription and purchase for the unconnected mode of operation.....	166
Figure 41 – Interactions for bulk download of service and programme keys	168
Figure 42 – Interactions for bulk download of purchase information	169
Figure 43 – Interactions for announcement of purchase items in service guide	170
Figure 44 – Interactions for pricing inquiry	171
Figure 45 – Interactions for unsuccessful purchase.....	175
Figure 46 – Interactions for successful purchase	179
Figure 47 – Interactions for subscription RO renewal and asynchronous charging	183
Figure 48 – Interactions for asynchronous charging and cancellation of open-ended subscriptions	184
Figure 49 – Interactions for acquisition and charging of tokens	188
Figure 50 – Samples of out-of-band purchase information displays for a registered device.....	209
Figure 51 – Sample of out-of-band purchase information displays for an unregistered device.....	210
Figure 52 – Example mapping of objects to RI stream packets.....	218
Figure 53 – Signalling of encrypted services and their associated key streams	232
Figure 54 – Signalling of encrypted services in the SDT.....	233
Figure 55 – Signalling of the rights issuer service in the SDT.....	234

Figure 56 – Addressing of a rights issuer service	234
Figure 57 – Signalling of purchase information via the SDT	235
Figure 58 – Signalling of purchase information via the CA_descriptor in the CAT	236
Figure 59 – Signalling of purchase information via the private data block of the CA_descriptor in the CAT	237
Figure 60 – Relationship between PCT, PIT, SBT and SDT	238
Figure 61 – Alternative usage of the purchase_item_descriptor in the SDT and EIT	239
Figure A.1 – Sample notification display	272
Figure A.2 – Conversion routes between modified julian date (MJD) and coordinated universal time (UTC)	275
Figure A.3 – Node numbering	280
Figure A.4 – AES for key derivation	281
Figure A.5 – Sample tree with correct node and device numbering	283
Figure A.6 – Computation of the TAA_report_code	288
Figure A.7 – Node numbering	293
Figure A.8 – Computation of the report_authentication_code	299
Figure A.9 – Relationship between DVB-T/C/S PSI/SI tables	312
Figure A.10 – Relationships between the defined types	314
Figure A.11 – XML fragment for SOC identifier	316
Figure A.12 – XML fragment for serviceBaseCID	316
Figure A.13 – Definition of UniversalPurchaseItemType	317
Figure A.14 – Definition of the ServiceBundleType	317
Figure A.15 – Definition of UniversalServiceInformationType	318
Figure A.16 – Definition of UniversalOnDemandServiceType	318
Figure A.17 – Definition of UniversalPurchaseType	319
Figure A.18 – Recording and super-distributing the recorded asset	329
Figure A.19 – Format of the OMADRMRecordingTimestamp	332
Figure A.20 – Format of the OMADRMRecordingInformationBlock	333
Figure A.21 – 18Crypt namespace declaration	334
Figure B.1 – Rights issuer communication with various types of devices in IPDC over DVB-H systems	356
Figure B.2 – Rights issuer communication with various types of devices in DVB-T/C/S systems	359
Figure B.3 – Rights issuer communication with various types of devices in IP systems	361
Figure B.4 – Purchase steps in case of an interactive device	362
Figure B.5 – Purchase steps in case of a broadcast device	364
Figure B.6 – Consumption steps from the broadcaster point of view	366
Figure B.7 – Consumption steps from the device point of view	367
Figure B.8 – Function blocks of service protection head-end	376
Figure B.9 – Systems and network elements of service protection head-end	378
Figure B.10 – IEC T/C/S components integrated into DVB SimulCrypt head-end	380
Figure B.11 – Locating 18Crypt KSM & BCRO as well as EMM & ECM	382
Figure B.12 – Carrying messages over the network	384
Figure B.13 – Sample network set-ups using the location descriptors	384

Figure B.14 – Expanding the IEC T/C/S head-end components	385
Figure B.15 – Deployment option A (combining DIST Mgmt and RI in SOC) – Local scenario.....	389
Figure B.16 – Deployment option A (combining DIST Mgmt and RI in SOC) – Roaming scenario.....	390
Figure B.17 – Deployment option B (combining SUB Mgmt and RI in COC) – Local scenario.....	392
Figure B.18 – Deployment option B (combining SUB Mgmt and RI in COC) – Roaming scenario.....	393
Figure B.19 – Scenarios 1 and 2 for bosb_masks	397
Figure B.20 – Scenarios 3 and 4 for bosb_masks	399
Figure B.21 – Scenarios 5 and 6 for bosb_masks	400
Figure B.22 – Scenarios 7 and 8 for bosb_masks	401
Figure B.23 – Scenarios 9 and 10 for bosb_masks (precedence)	402
Figure B.24 – Diagram of keyset_block, sessionkey_block and surplus_block.....	404
Table 1 – Supported systems and device types	34
Table 2 – Keyset in the registration data	44
Table 3 – Definition of transport_scrambling_control bits	62
Table 4 – Definition of pes_scrambling_control field bits	62
Table 5 – Descrambling possibility matrix	64
Table 6 – Supported ciphers for MPEG2 TS Crypt	64
Table 7 – Format of key stream message	66
Table 8 – Descriptors for access_criteria_descriptor_loop	68
Table 9 – Access_criteria_descriptors.....	68
Table 10 – Parental_rating access criteria descriptor	68
Table 11 – Parental rating values for each parental rating type	69
Table 12 – Copy_control_information access criteria descriptor	70
Table 13 – Bit assignments of copy_control_information_byte	71
Table 14 – CCI bit assignments	71
Table 15 – EMI values and content	71
Table 16 – APS value definitions	71
Table 17 – CIT values and application	72
Table 18 – RCT values and application.....	72
Table 19 – Blackout_spotbeam access criteria descriptor	73
Table 20 – Operator field values and their meaning	73
Table 21 – Constants in key stream message	75
Table 22 – Content_key_index options	77
Table 23 – cipher_mode options	78
Table 24 – Obtaining the content key	79
Table 25 – Traffic key lifetime	80
Table 26 – Values of permissions_category and their meaning	81
Table 27 – Format of BCRO.....	85
Table 28 – Address_mode	87

Table 29 – Asset format	89
Table 30 – Asset_type	90
Table 31 – Mapping of address_mode to keys	90
Table 32 – Mapping of address_mode to keys	91
Table 33 – Mapping of address_mode to keys	91
Table 34 – Permission format	92
Table 35 – Action format	93
Table 36 – Action_type	93
Table 37 – Constraint format	94
Table 38 – Format of constraint_descriptor	94
Table 39 – Constraint_tag	95
Table 40 – Format of count_constraint_descriptor	95
Table 41 – Format of timed_count_constraint_descriptor	95
Table 42 – Format of datetime_constraint_descriptor	96
Table 43 – Format of interval_constraint_descriptor	97
Table 44 – Format of accumulated_constraint_descriptor	97
Table 45 – Format of individual_constraint_descriptor	98
Table 46 – Id_type	98
Table 47 – Format of system_constraint_descriptor	98
Table 48 – Format of token_management_constraint_descriptor	99
Table 49 – Registration types	101
Table 50 – NSD action request code fields	104
Table 51 – NSD action types	105
Table 52 – Token consumption data	107
Table 53 – TAA report data	108
Table 54 – Messages of the 1-pass IRD protocol	110
Table 55 – UDN explanation	112
Table 56 – Major industry identifier	113
Table 57 – longform_udn	113
Table 58 – Notify device data message parameters	114
Table 59 – Device data	114
Table 60 – Message fields	115
Table 61 – Status values	116
Table 62 – Fields of certificate_version parameter	116
Table 63 – Allowed values for ri_certificate_counter	117
Table 64 – Allowed values for obsp_response_counter	118
Table 65 – Values for flags signalling data absent/data present	118
Table 66 – Allowed values for subscriber_group_key_flag	119
Table 67 – Values and their meaning for signature_type_flag	119
Table 68 – Message syntax	124
Table 69 – Message fields	126
Table 70 – Status values	127
Table 71 – Fields of certificate_version parameter	127

Table 72 – Message syntax	129
Table 73 – Message fields	130
Table 74 – Status values	130
Table 75 – Message syntax	131
Table 76 – Message fields	132
Table 77 – Status values	132
Table 78 – Fields of certificate_version parameter	133
Table 79 – Message syntax	134
Table 80 – Format of contact object	135
Table 81 – Contact_type	135
Table 82 – Encoding rules for contactdata	136
Table 83 – Off-line protocols (from device to RI)	137
Table 84 – 1-pass protocols (from RI to device)	137
Table 85 – Protocol interrelation	137
Table 86 – Message fields	138
Table 87 – Status values	139
Table 88 – Fields of certificate_version parameter	139
Table 89 – Message syntax	144
Table 90 – Message fields	145
Table 91 – Status values	146
Table 92 – Fields of certificate_version parameter	146
Table 93 – Message syntax	148
Table 94 – Message syntax	150
Table 95 – Offline protocols (from device to RI)	151
Table 96 – 1-pass protocols (from RI to device)	151
Table 97 – Protocol interrelation	151
Table 98 – Fields of token delivery response message	152
Table 99 – Address_mode for token delivery response message	153
Table 100 – Message error codes	154
Table 101 – Mapping of address_mode to keys for the token delivery response message	156
Table 102 – Mapping of address_mode to keys for the token delivery response message	156
Table 103 – Syntax of token delivery response message	157
Table 104 – Requirements for the support of RI services and streams by IPDC over DVB-H devices	161
Table 105 – Requirements for the support of rights issuer services and streams by service providers in IPDC over DVB-H systems	162
Table 106 – Definition of mandatory SOC attributes in request/response messages	190
Table 107 – Occurrence of error codes in response messages	192
Table 108 – Data to be provided to the customer operation centre	209
Table 109 – Traffic layer options for transmission over IPDC over DVB-H	215
Table 110 – Format of the rights issuer stream	219
Table 111 – Traffic layer options for transmission over MPEG2 TS-based networks	225

Table 112 – KSM table	225
Table 113 – BCRO table	227
Table 114 – Carrying registration layer messages via MPEG sections in T/C/S system	228
Table 115 – Syntax of registration message table (RMT)	229
Table 116 – Purchase channel table	240
Table 117 – Service bundle table	244
Table 118 – Purchase item table	247
Table 119 – Private descriptor tags used for 18Crypt	248
Table 120 – Possible locations of descriptors	249
Table 121 – Service_ID_descriptor	249
Table 122 – Right issuer ID descriptor	250
Table 123 – Purchase info location descriptor	251
Table 124 – Purchase item descriptor	253
Table 125 – Subscription_type values	254
Table 126 – Example price with different decimal point location values	255
Table 127 – Provider name descriptor	256
Table 128 – Eurocrypt addressing descriptor	256
Table 129 – Address_mode	257
Table 130 – Info URL descriptor	258
Table 131 – Key URL descriptor	258
Table 132 – Linkage descriptor	259
Table 133 – Linkage type coding	260
Table 134 – IP linkage descriptor	260
Table 135 – User defined IDs	262
Table 136 – Additions to the broadcast discovery record	265
Table 137 – Additions to the content-on-demand discovery record	266
Table 138 – Sequence of events for purchase and supply of a content-on-demand item	268
Table 139 – Traffic layer options for transmission over non-MPEG2 TS based IP networks	269
Table A.1 – Status/error codes	273
Table A.2 – Local time offset coding	277
Table A.3 – Standard keyset with RSA block size 1024	278
Table A.4 – Standard keyset with other RSA block sizes	279
Table A.5 – Extended keyset with RSA block size 1024	279
Table A.6 – Extended keyset with other RSA block sizes	280
Table A.7 – Error likelihood in human communication	288
Table A.8 – Defined tag values	292
Table A.9 – Defined length values	294
Table A.10 – Correct usage of length values	294
Table A.11 – TAA descriptor syntax	296
Table A.12 – TAA algorithm values	296
Table A.13 – Message_tag overview	297
Table A.14 – Table ID overview	297

Table A.15 – Multilingual text structure	298
Table A.16 – Mapping of required service guide data to the IPDC ESG.....	309
Table A.17 – Mapping of required service guide data to DVB PSI/SI tables.....	311
Table A.18 – Mapping of required service guide data to IPI BCG/TV anytime.....	314
Table A.19 – Updated permission element.....	326
Table A.20 – Access element.....	328
Table A.21 – Semantics of the save element	330
Table A.22 – Use of programme and service keys.....	330
Table A.23 – Fields in the GroupID box.....	331
Table A.24 – CommonHeaders box fields	331
Table A.25 – Conformance table for IPDC over DVB-H systems	343
Table A.26 – Conformance table for DVB-T/C/S systems	347
Table A.27 – Conformance table for IPTV systems	350
Table B.1 – Messages involved in IEC T/C/S systems.....	379
Table B.2 – Reference overview information	383
Table B.3 – Example 1: CGF with cities and regions	396
Table B.4 – Example 2: CGF with sports and regions (independent)	396
Table B.5 – Example 3: CGF with sports and regions (overlapping)	398
Table B.6 – Category of references.....	405

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INTERNET PROTOCOL (IP) AND TRANSPORT STREAM (TS) BASED SERVICE ACCESS

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62455 has been prepared by technical area 1: Terminals for audio, video and data services and content, of IEC technical committee 100: Audio, video and multimedia systems and equipment.

This second edition cancels and replaces the first edition, published in 2007, and constitutes a technical revision.

The main changes with respect to the previous edition are listed below.

- Recent developments in DVB and OMA standards caused some incompatibilities, which have been solved in the second edition.
- Technical errors have been corrected, missing details added.
- References have been updated to the newest available ones.
- In addition, a number of editorial corrections and readability improvements have been made, where the original text could have lead to misunderstanding due to unclear wording or the use of slightly different spellings for the same item.

The text of this standard is based on the following documents:

CDV	Report on voting
100/1551/CDV	100/1627/RVC

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

The committee has decided that the contents of this publication will remain unchanged until the stability date indicated on the IEC web site under "<http://webstore.iec.ch>" in the data related to the specific publication. At this date, the publication will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTERNET PROTOCOL (IP) AND TRANSPORT STREAM (TS) BASED SERVICE ACCESS

1 Scope

This International Standard specifies the terminal for a service purchase and protection system for digital broadcasts, called the 18Crypt system. It is applicable in all countries and regions with suitably compliant broadcasting and multimedia distribution systems. Guidelines for compatible broadcast services are given in this standard. The service purchase and protection functions operate in a pure broadcast environment that may be combined with a bi-directional interactivity channel.

This standard is applicable to the following broadcast systems.

a) IP datacast over DVB-H systems

IP datacast over DVB-H is an end-to-end broadcast system for delivery of any type of digital content and services using IP-based mechanisms optimized for devices with limitations on computational resources and battery. An inherent part of the IP datacast system is that it comprises a unidirectional DVB broadcast path that may be combined with a bi-directional mobile/cellular interactivity path. IP datacast is thus a platform that can be used for enabling the convergence of services from broadcast/media and telecommunications domains (for example, mobile/cellular). This standard specifies service purchase and protection for IP datacast over DVB-H systems (see Table B.6 for an overview of references to one such system).

b) DVB T/C/S systems

DVB T/C/S systems are end-to-end broadcast systems for audio/video data that employ an MPEG2 transport stream and use terrestrial, cable or satellite broadcast networks. This standard specifies a system for the protection of these broadcasts in a pure broadcast environment. In addition, this standard specifies how purchasing, key management and registration may be carried out over an optional interactivity channel. The protection technologies offered by this standard are designed to operate within an existing DVB SimulCrypt environment (see Table B.6 for an overview of references).

c) MPEG2 TS-based IP systems

MPEG2 TS-based IP systems employ bi-directional IP networks for the (broadcast) delivery of MPEG2 transport streams. This standard specifies a system for the purchase and protection of services and content delivered via these networks. This standard is applicable to, for example, DVB-IPI systems (see Table B.6 for an overview of references).

d) Non-MPEG2 TS-based IP systems

Non-MPEG2 TS-based IP systems employ bi-directional IP networks for the (broadcast) delivery of audio/video or other data using IP protocols instead of an MPEG2 transport stream. This standard specifies a system for the purchase and protection of services and content delivered via these networks (see Table B.6 for an overview of references).

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 8859-1:1998, *Information technology – 8-bit single-byte coded graphic character sets – Part 1: Latin alphabet No. 1*

ISO/IEC 13818-1:2007, *Information technology – Generic coding of moving pictures and associated audio information: Systems*

ISO/IEC 14496-12:2008, *Information technology – Coding of audio-visual objects – Part 12: ISO base media file format*

ISO/IEC 15938-5:2003, *Information technology – Multimedia content description interface – Part 5: Multimedia description schemes*

ISO 639-1:2002, *Codes for the representation of names of languages – Part 1: Alpha-2 code*

ISO 639-2:1998, *Codes for the representation of names of languages – Part 2: Alpha-3 code*

ISO 3166 (all parts), *Codes for the representation of names of countries and their subdivisions*

ISO 4217, *Codes for the representation of currencies and funds*

ISO 8601:2004, *Data elements and interchange formats – Information interchange – Representation of dates and times*

ETSI EN 102 034, *Digital Video Broadcasting (DVB) – Transport of MPEG-2-based DVB services over I- based networks*

ETSI EN 300 468, *Digital Video Broadcasting (DVB) – Specification for Service Information (SI) in DVB systems*

ETSI EN 301 192, *Digital Video Broadcasting (DVB) – DVB specification for data broadcasting*

ETSI EN 302 304, *Digital Video Broadcasting (DVB) – Transmission system for handheld terminals (DVB-H)*

ETSI TS 102 539, *Digital Video Broadcasting (DVB) – Carriage of broadband content guide (BCG) information over internet protocol (IP)*

ETSI ETR 162, http://www.dvb.org/products_registration/dvb_identifiers/(this website replaces ETR 162)

ETSI ETR 289, *Digital Video Broadcasting (DVB) – Support for use of scrambling and conditional access (CA) within digital broadcasting systems*

ETSI TS 102 471, *Digital Video Broadcasting (DVB) – IP datacast over DVB-H: Electronic service guide (ESG)*

ETSI TS 102 472, *Digital Video Broadcasting (DVB) – IP datacast over DVB-H: Content delivery protocols*

ETSI TS 102 822-3-1, *Broadcast and on-line services: Search, select, and rightful use of content on personal storage systems (TV-anytime) – Part 3: Metadata – Sub-part 1: Phase 1 – Metadata schemas*

ETSI TS 103 197, *Digital Video Broadcasting (DVB) – SimulCrypt Head-end implementation of DVB SimulCrypt, v1.4.1*

SOMMAIRE

AVANT-PROPOS	423
1 Domaine d'application	425
2 Références normatives	426
3 Termes, définitions et abréviations	427
3.1 Termes et définitions	427
3.2 Symboles	433
3.3 Abréviations	434
3.4 Identifiants assignés par des entités externes	439
4 Généralités	439
4.1 Vue d'ensemble	439
4.2 Description générale du système et de ses éléments	439
4.2.1 Généralités	439
4.2.2 Technologies sélectionnées	440
4.2.3 Vue générale du modèle à quatre couches pour la protection des services	442
4.3 Système de bout en bout	444
4.4 Systèmes et types de dispositifs pris en charge	445
4.5 Protection de service et protection de contenu	446
5 Spécifications générales	447
5.1 Architecture de bout en bout	447
5.2 Cas spéciaux	449
5.2.1 Services en transmission libre	449
5.2.2 Services en vision libre	449
5.3 Guide de service et achat de services	449
5.4 Modèle à quatre couches – Hiérarchie des clés	451
5.4.1 Généralités	451
5.4.2 Clés sur la couche trafic	451
5.4.3 Clés sur la couche de séquence de clé	451
5.4.4 Clés sur la couche gestion des droits (mode interactif)	454
5.4.5 Clés sur la couche gestion des droits (mode diffusion)	454
5.4.6 Clés sur la couche inscription (mode interactif)	455
5.4.7 Clés sur la couche inscription (mode diffusion)	455
5.4.8 Vue générale de l'authentification	458
5.5 Déploiement pour le mode de fonctionnement en diffusion	459
5.5.1 Concept de domaines – Domaines interactifs et de diffusion	459
5.5.2 Adressage (groupe/sous-ensemble/dispositif/domaine)	460
5.5.3 Schéma de chiffrement de diffusion sans message	463
6 Couche trafic	465
6.1 Généralités	465
6.2 IPsec	465
6.2.1 Généralités	465
6.2.2 Sélecteurs	467
6.2.3 Protocole et mode d'encapsulation	467
6.2.4 Algorithme de chiffrement	467
6.2.5 Algorithme d'authentification	467
6.2.6 Gestion de l'association de sécurité	467
6.3 ISMACryp	468

6.3.1	Contenu transmis en continu	468
6.3.2	Contenu audio/visuel téléchargeable (stocké sur des fichiers MP4)	468
6.3.3	Utilisation de ISMACryp avec les couches de gestion des droits et de séquence de clé	469
6.4	SRTP	470
6.4.1	Généralités	470
6.4.2	Gestion des clés	472
6.4.3	Algorithme de chiffrement	472
6.4.4	Algorithme d'authentification	472
6.5	MPEG2 TS crypt	473
6.5.1	Généralités	473
6.5.2	Embrouillage au niveau du flux de transport	474
6.5.3	Embrouillage au niveau du flux PES	475
6.5.4	Désembrouillage de contenu MPEG2	475
6.5.5	Chiffres pris en charge	476
6.5.6	Gestion des clés	477
7	Couche de séquence de clé	478
7.1	Généralités	478
7.2	Format du message de séquence de clé (KSM)	478
7.2.1	Format	478
7.2.2	Descripteurs pour access_criteria_descriptor_loop (boucle de description des critères d'accès)	480
7.2.3	Constantes	488
7.2.4	Codage et sémantique des attributs	488
8	Couche de gestion des droits	497
8.1	Généralités	497
8.2	Identification des objets de droits	497
8.3	Exigences pour les objets de droits	498
8.3.1	Exigences pour les RO d'accès au service	498
8.3.2	Exigences pour les RO d'accès au programme	499
8.4	Format des objets de droits	499
8.4.1	Format d'un objet de droits pour un canal d'interactivité (ICRO)	499
8.4.2	Format d'un objet de droits d'accès à un contenu porté par un canal de diffusion (BCRO)	499
8.4.3	Format de l'objet asset (actif)	503
8.4.4	Format de l'objet 'permission'	506
8.4.5	Format de l'objet action	507
8.4.6	Format de l'objet contraint	508
9	Couche inscription	514
9.1	Généralités	514
9.2	Contexte de RI	514
9.3	Protocoles et spécification des messages de la couche inscription	515
9.3.1	Spécification de la couche inscription avec canal d'interactivité	515
9.3.2	Spécification de la couche inscription avec canal de diffusion	515
9.3.3	Entrée et sortie de domaine	554
9.3.4	Gestion des jetons	570
9.3.5	Inscription en mode mixte pour les modes de fonctionnement interactif et de diffusion	577
10	Signalisation et guide de service	579

10.1	Généralités	579
10.2	Exigences de signalisation	579
10.2.1	Informations de signalisation	579
10.2.2	Exigences de signalisation du KSM	579
10.2.3	Exigences de signalisation des services	580
10.3	Exigences du guide de service	580
10.4	Recommandations pour le guide de service	580
11	Services d'émetteurs de droits et flux d'émetteurs de droits	580
11.1	Généralités	580
11.2	Services d'émetteur de droits	581
11.2.1	Exigences pour les services d'émetteurs de droits dans les systèmes IPDC sur DVB-H	581
11.2.2	Exigences pour les services d'émetteurs de droits dans les systèmes DVB-T/C/S	581
11.2.3	Exigences pour la prise en charge des services et des flux d'émetteur de droits dans les systèmes IPTV	582
11.3	Utilisation des flux et des services d'émetteur de droits	582
11.3.1	Généralités	582
11.3.2	Flux de RI planifié	583
11.3.3	Flux de RI <i>ad hoc</i>	583
11.3.4	Flux de RI intrabande dans un service multimédia	583
12	Abonnement et achat de services	584
12.1	Généralités	584
12.2	Achat sur un canal d'interactivité	588
12.2.1	Généralités	588
12.2.2	Séquences d'achat types	588
12.2.3	Protocole	607
12.2.4	Schémas XML pour les messages de requête et de réponse	608
12.2.5	Définition du schéma XML pour les éléments XML relatifs aux requêtes et aux réponses	624
12.3	Achat pour les dispositifs en mode mixte	628
12.4	Achat hors bande	629
12.4.1	Moyens d'achat – Introduction	629
12.4.2	Achat hors bande à partir des données du guide de service	629
12.5	Informations exigées du guide de service	631
12.5.1	Généralités	631
12.5.2	Centre d'exploitation des services (comprenant la gestion de distribution des services)	632
12.5.3	Centre d'exploitation client (comprenant la gestion d'abonnement aux services)	632
12.5.4	Service	633
12.5.5	Elément de planification (ScheduleItem)	634
12.5.6	Elément de contenu (ContentItem)	634
12.5.7	Elément d'achat (PurchaseItem)	635
12.5.8	Données d'achat	635
13	Protection des systèmes IPDC sur DVB-H	636
13.1	Généralités	636
13.2	Distribution des données de couche trafic des systèmes IPDC sur DVB-H	636
13.3	Distribution des données de flot de chiffrement des systèmes IPDC sur DVB- H	636

13.4	Distribution des données de gestion des droits des systèmes IPDC sur DVB-H	636
13.4.1	Généralités	636
13.4.2	Distribution d'ICRO dans les systèmes IPDC sur DVB-H sur un canal d'interactivité	636
13.4.3	Distribution d'ICRO dans les systèmes IPDC sur DVB-H sur un canal de diffusion.....	637
13.5	Distribution des données d'inscription dans les systèmes IPDC sur DVB-H.....	637
13.5.1	Généralités	637
13.5.2	Distribution des données d'inscription dans les systèmes IPDC sur DVB-H sur un canal d'interactivité	637
13.5.3	Distribution des données d'inscription dans les systèmes IPDC sur DVB-H sur un canal de diffusion	637
13.6	Signalisation et guides de service dans les systèmes IPDC sur DVB-H.....	637
13.6.1	Généralités	637
13.6.2	Signalisation du KSM dans les systèmes IPDC sur DVB-H	637
13.6.3	Le guide de service les systèmes IPDC sur DVB-H.....	638
13.7	Format et utilisation de flux de RI dans les systèmes IPDC sur DVB-H	639
13.7.1	Généralités	639
13.7.2	Caractéristiques IP	639
13.7.3	Format du paquet du flux de RI.....	640
13.7.4	Notes de mise en œuvre.....	642
13.7.5	Mappage des messages pour les services et les flux de RI.....	642
13.7.6	Découvertes de services de RI, de flux et des informations de planification	643
13.7.7	Mises à jour de la chaîne de certificat.....	644
13.7.8	Renvoi des BCRO	644
13.7.9	Récapitulatif des exigences pour les émetteurs de droits	645
13.7.10	Récapitulatif des exigences pour les dispositifs	646
13.7.11	Mappage des messages pour les rafales DVB-H en tranches de temps	646
14	Protection des systèmes DVB T/C/S.....	647
14.1	Généralités	647
14.2	Distribution des données de couche trafic dans les systèmes DVB T/C/S	647
14.3	Distribution des données de flots de chiffrement dans les systèmes DVB T/C/S	647
14.4	Distribution des données de gestion des droits dans les systèmes DVB T/C/S	648
14.4.1	Généralités	648
14.4.2	Distribution d'ICRO dans les systèmes DVB T/C/S sur un canal d'interactivité	648
14.4.3	Distribution de BCRO dans les systèmes DVB T/C/S sur un canal de diffusion.....	649
14.5	Distribution des données d'inscription dans les systèmes DVB T/C/S.....	650
14.5.1	Généralités	650
14.5.2	Distribution de données d'inscription dans les systèmes DVB T/C/S sur un canal d'interactivité	650
14.5.3	Distribution de données d'inscription dans les systèmes DVB T/C/S sur un canal de diffusion.....	650
14.5.4	Table de message d'inscription.....	651
14.6	Signalisation et guide de service dans les systèmes DVB T/C/S	653
14.6.1	Généralités	653

14.6.2	Signalisation des services chiffrés dans les systèmes DVB T/C/S.....	654
14.6.3	Tables SI.....	664
14.6.4	Descripteurs SI.....	672
14.7	Identifiants définis par l'utilisateur utilisés dans les tables DVB-SI.....	686
14.8	Portée des identifiants utilisés dans les tables DVB-SI.....	686
14.9	Format des services de RI dans les systèmes DVB T/C/S.....	687
14.9.1	Généralités.....	687
14.9.2	Format du paquet du flux de RI.....	687
14.9.3	Adressage d'objets.....	687
14.9.4	Mappage des messages pour les services et les flux de RI.....	687
15	Protection des systèmes IP fondés sur TS MPEG2.....	688
15.1	Généralités.....	688
15.2	Encapsulation d'un TS MPEG2 en IP.....	688
15.3	Distribution des données de couche trafic dans les systèmes IP fondés sur TS MPEG2.....	688
15.4	Distribution des données de flot de chiffrement dans les systèmes IP fondés sur TS MPEG2.....	688
15.5	Distribution des données de gestion des droits dans les systèmes IP fondés sur TS MPEG2.....	688
15.6	Distribution des données d'inscription dans les systèmes IP fondés sur TS MPEG2.....	689
15.7	Signalisation et guides de service dans les systèmes IP fondés sur TS MPEG2.....	689
15.7.1	Généralités.....	689
15.7.2	Signalisation et guide de service dans les systèmes DVB-IPI.....	689
15.7.3	Signalisation et guides de service dans les systèmes non conformes à DVB-IPI.....	691
15.8	Format des services de RI sur les systèmes IP fondés sur TS MPEG2.....	692
15.9	Prise en charge du contenu à la demande.....	692
15.9.1	Généralités.....	692
15.9.2	Prise en charge de lecture rapide de contenu à la demande.....	693
15.10	Utilisation d'interfaces d'achat du côté serveur.....	694
15.10.1	Généralités.....	694
15.10.2	Exemple d'inscription à travers une interface en ligne.....	694
15.10.3	Exemple d'achat à travers une interface en ligne.....	694
16	Protection des systèmes IP non fondés sur TS MPEG2.....	695
16.1	Généralités.....	695
16.2	Distribution des données de couche trafic dans les systèmes IP non fondés sur TS MPEG2.....	695
16.3	Distribution des données de flot de chiffrement dans les systèmes IP non fondés sur TS MPEG2.....	695
16.4	Distribution des données de gestion des droits dans les systèmes IP non fondés sur TS MPEG2.....	695
16.5	Distribution des données d'inscription dans les systèmes IP non fondés sur TS MPEG2.....	695
16.6	Signalisation et guides de service dans les systèmes IP non fondés sur TS MPEG2.....	695
16.7	Format des services de RI sur les systèmes IP non fondés sur TS MPEG2.....	696
16.8	Prise en charge du contenu à la demande.....	696
Annexe A (normative)	Spécifications de prise en charge.....	697
Annexe B (informative)	Considérations relatives au déploiement.....	785

Bibliographie.....	838
Figure 1 – Vue générale du système.....	440
Figure 2 – Protection des services par le modèle à quatre couches.....	442
Figure 3 – Vue très simplifiée du système de bout en bout.....	444
Figure 4 – Protection de service / protection de contenu.....	446
Figure 5 – Entités de protection et d'achat de services et leurs noms (architecture de diffusion).....	447
Figure 6 – Infrastructure à clé publique.....	448
Figure 7 – Vue générale du guide de service et de l'achat.....	450
Figure 8 – Hiérarchie de clés à 4 couches – utilisation de SEK uniquement.....	452
Figure 9 – Hiérarchie de clés à 4 couches – utilisation de PEK et SEK.....	454
Figure 10 – Hiérarchie de l'authentification.....	458
Figure 11 – Explication du concept d'adressage.....	460
Figure 12 – BCRO (très simplifié) de groupe.....	461
Figure 13 – BCRO (très simplifié) de groupe d'abonnés.....	461
Figure 14 – BCRO (très simplifié) de dispositif unique.....	462
Figure 15 – BCRO (très simplifié) de domaine de diffusion.....	462
Figure 16 – Exemple d'arbre sans message avec trois nœuds (clés).....	464
Figure 17 – Éléments de l'association de sécurité IPsec.....	466
Figure 18 – Gestion des clés ISMACryp.....	469
Figure 19 – Gestion du contexte cryptographique SRTP.....	471
Figure 20 – Gestion du contexte cryptographique de flux de transport MPEG2.....	473
Figure 21 – Comparaison des TS à clé simple et à clé double dans le temps.....	476
Figure 22 – Inscription pour le mode de fonctionnement en diffusion avec une ROT.....	516
Figure 23 – Protocole NDD hors ligne.....	517
Figure 24 – Exemples d'affichages de notification.....	518
Figure 25 – Protocole NSD hors ligne.....	518
Figure 26 – Code de requête d'action (ARC).....	518
Figure 27 – Exemples d'affichages de notification représentant un message ARC.....	520
Figure 28 – Exemple d'affichage de notification de rapport de consommation de jetons.....	521
Figure 29 – Exemple d'affichage de rapport TAA.....	523
Figure 30 – Protocole PDR 1 passe – (première) inscription de dispositif.....	523
Figure 31 – Protocole IRD à 1 passe – Message à destination du dispositif initié par le RI (ici: réinscription).....	524
Figure 32 – Numéro de dispositif unique (UDN).....	527
Figure 33 – Message device_registration_response().....	538
Figure 34 – Structure du message device_registration_response().....	540
Figure 35 – Message domain_registration_response().....	560
Figure 36 – Structure du message domain_registration_response().....	561
Figure 37 – Inscription pour le mode de fonctionnement mixte avec une ROT.....	578
Figure 38 – Relation entre le service et de RI et le flux de RI et les autres services et flux de RI.....	583

Figure 39 – Flux de messages pour d'abonnement et d'achat de services pour le mode de fonctionnement connecté	586
Figure 40 – Flux de messages pour d'abonnement et d'achat de services pour le mode de fonctionnement non connecté	588
Figure 41 – Interactions pour le téléchargement en vrac de clés de service et de programme	590
Figure 42 – Interactions pour le téléchargement en vrac d'informations d'achat	591
Figure 43 – Interactions pour l'annonce des éléments d'achat dans le guide de service	592
Figure 44 – Interactions pour la demande de tarification	593
Figure 45 – Interactions pour l'échec de l'achat	596
Figure 46 – Interactions pour la réussite de l'achat	600
Figure 47 – Interactions pour le renouvellement du RO d'abonnement et la facturation asynchrone	603
Figure 48 – Interactions pour la facturation asynchrone et l'annulation des abonnements renouvelables	604
Figure 49 – Interactions pour l'acquisition et la facturation de jetons	607
Figure 50 – Exemples d'affichage d'informations d'achat hors bande pour un dispositif inscrit	631
Figure 51 – Exemples d'affichage d'informations d'achat hors bande pour un dispositif non inscrit	631
Figure 52 – Exemple de mappage d'objets pour des paquets de flux de RI	640
Figure 53 – Signalisation des services chiffrés et de leurs flots de chiffrement associés	655
Figure 54 – Signalisation de services chiffrés dans la SDT	656
Figure 55 – Signalisation de services d'émetteur de droits dans la SDT	657
Figure 56 – Adressage d'un service d'émetteur de droits	658
Figure 57 – Signalisation des informations d'achat par la SDT	659
Figure 58 – Signalisation des informations d'achat à travers le CA_descriptor dans la CAT	660
Figure 59 – Signalisation des informations d'achat à travers le bloc de données privées du CA_descriptor dans la CAT	661
Figure 60 – Relation entre PCT, PIT, SBT et SDT	662
Figure 61 – Utilisation alternative du purchase_item_descriptor dans la SDT et l'EIT	663
Figure A.1 – Exemple d'affichage de notification	699
Figure A.2 – Conversion entre les Jours juliens modifiés (MJD) et le Temps universel coordonné (UTC)	701
Figure A.3 – Numérotation des nœuds	707
Figure A.4 – AES pour dérivation des clés	707
Figure A.5 – Exemple d'arbre avec numérotation correcte des nœuds et des dispositifs	709
Figure A.6 – Calcul du TAA_report_code	714
Figure A.7 – Numérotation des nœuds	720
Figure A.8 – Calcul du report_authentication_code	726
Figure A.9 – Relations entre les tables PSI/SI DVB-T/C/S	740
Figure A.10 – Relations entre les types définis	741
Figure A.11 – Fragment XML pour l'identifiant du SOC	743
Figure A.12 – Fragment XML pour le serviceBaseCID	743
Figure A.13 – Définition de UniversalPurchaseItemType	744

Figure A.14 – Définition de ServiceBundleType	745
Figure A.15 – Définition de UniversalServiceInformationType	745
Figure A.16 – Définition de UniversalOnDemandServiceType	746
Figure A.17 – Définition de UniversalPurchaseType.....	746
Figure A.18 – Enregistrement et super distribution de l'actif enregistré	757
Figure A.19 – Format du OMADRMRecordingTimestamp	760
Figure A.20 – Format du OMADRMRecordingInformationBlock	761
Figure A.21 – Déclaration de l'espace de nom 18Crypt	763
Figure B.1 – Communication de l'émetteur de droits avec différents types de dispositifs dans les systèmes IPDC sur DVB-H.....	787
Figure B.2 – Communication de l'émetteur de droits avec différents types de dispositifs dans les systèmes DVB-T/C/S	790
Figure B.3 – Communication de l'émetteur de droits avec différents types de dispositifs dans les systèmes IP	792
Figure B.4 – Etapes d'achat dans le cas d'un dispositif interactif.....	793
Figure B.5 – Etapes d'achat dans le cas d'un dispositif de diffusion	795
Figure B.6 – Etapes de consommation du point de vue du diffuseur.....	797
Figure B.7 – Etapes de consommation du point de vue du dispositif	798
Figure B.8 – Blocs fonctionnels de la tête du réseau de protection des services	807
Figure B.9 – Systèmes et éléments de réseau d'une tête de réseau de protection des services	809
Figure B.10 – Composants IEC T/C/S intégrés dans la tête de réseau DVB SimulCrypt.....	811
Figure B.11 – Localisation des KSM et BCRO ainsi que des EMM et ECM 18Crypt.....	813
Figure B.12 – Transport des messages sur le réseau.....	815
Figure B.13 – Exemples d'installation de réseaux utilisant les descripteurs de localisation	815
Figure B.14 – Extension des composants de tête de réseau IEC T/C/S.....	816
Figure B.15 – Option de déploiement A (combinant DIST Mgmt et RI dans le SOC) – Scénario local.....	820
Figure B.16 – Option de déploiement A (combinant DIST Mgmt et RI dans le SOC) – Scénario d'itinérance	822
Figure B.17 – Option de déploiement B (combinant SUB Mgmt et RI dans le COC) – Scénario local.....	824
Figure B.18 – Option de déploiement B (combinant SUB Mgmt et RI dans le COC) – Scénario d'itinérance	825
Figure B.19 – Scénarios 1 et 2 pour les bosb_masks	829
Figure B.20 – Scénarios 3 et 4 pour les bosb_masks	831
Figure B.21 – Scénarios 5 et 6 pour les bosb_masks	832
Figure B.22 – Scénarios 7 et 8 pour les bosb_masks	833
Figure B.23 – Scénarios 9 et 10 pour les bosb_masks (priorité).....	834
Figure B.24 – Schéma des blocs keyset_block, sessionkey_block et surplus_block	836
Tableau 1 – Systèmes et types de dispositifs pris en charge.....	445
Tableau 2 – Clés des données d'inscription	455
Tableau 3 – Définition des bits transport_scrambling_control.....	474
Tableau 4 – Définition des bits du champ pes_scrambling_control.....	475

Tableau 5 – Matrice des possibilités de désembrouillage	476
Tableau 6 – Chiffres pris en charge pour MPEG2 TS Crypt.....	477
Tableau 7 – Format du message de séquence de clé.....	478
Tableau 8 – Descripteurs pour access_criteria_descriptor_loop.....	480
Tableau 9 – Access_criteria_descriptors.....	480
Tableau 10 – Descripteur de critère d'accès Parental_rating.....	481
Tableau 11 – Valeurs de l'autorisation parentale pour chaque type d'autorisation parentale	481
Tableau 12 – Descripteur de critère d'accès Copy_control_information.....	483
Tableau 13 – Attribution de bits à l'octet copy_control_information_byte.....	483
Tableau 14 – Attribution de bits CCI	483
Tableau 15 – Valeurs EMI et contenu	484
Tableau 16 – Définitions des valeurs APS.....	484
Tableau 17 – Valeurs CIT et application	484
Tableau 18 – Valeurs RCT et application	485
Tableau 19 – Descripteur de critère d'accès blackout_spotbeam	485
Tableau 20 – Valeurs du champ operator et leur signification	486
Tableau 21 – Constantes dans le message de séquence de clé.....	488
Tableau 22 – Options de content_key_index.....	491
Tableau 23 – Options de cipher_mode.....	491
Tableau 24 – Obtention de la clé de contenu	493
Tableau 25 – Durée de vie de la clé de trafic.....	493
Tableau 26 – Valeurs de permissions_category et leur signification.....	495
Tableau 27 – Format de BCRO	500
Tableau 28 – Address_mode	501
Tableau 29 – Format de l'objet asset	503
Tableau 30 – Asset_type	504
Tableau 31 – Mappage de address_mode pour les clés	505
Tableau 32 – Mappage de address_mode pour les clés	505
Tableau 33 – Mappage de address_mode pour les clés	506
Tableau 34 – Format de permission	506
Tableau 35 – Format de l'objet action	507
Tableau 36 – Action_type	507
Tableau 37 – Format de l'objet constraint	508
Tableau 38 – Format de constraint_descriptor	509
Tableau 39 – Constraint_tag.....	509
Tableau 40 – Format de count_constraint_descriptor.....	509
Tableau 41 – Format de timed_count_constraint_descriptor	510
Tableau 42 – Format de datetime_constraint_descriptor	510
Tableau 43 – Format de interval_constraint_descriptor	511
Tableau 44 – Format de accumulated_constraint_descriptor.....	511
Tableau 45 – Format de individual_constraint_descriptor.....	512
Tableau 46 – Id_type	512

Tableau 47 – Format de system_constraint_descriptor	513
Tableau 48 – Format de token_management_constraint_descriptor	513
Tableau 49 – Types d'inscriptions	515
Tableau 50 – Champs du code de requête d'action NSD	519
Tableau 51 – Types d'actions NSD	519
Tableau 52 – Données de consommation de jetons	521
Tableau 53 – Données de rapport TAA	523
Tableau 54 – Messages du protocole IRD 1 passe	525
Tableau 55 – Explication de l'UDN	528
Tableau 56 – Indicateur de la principale activité économique	528
Tableau 57 – longform_udn	529
Tableau 58 – Paramètres du message de données de notification du dispositif	529
Tableau 59 – Données de dispositif	530
Tableau 60 – Champs du message	531
Tableau 61 – Valeurs du paramètre status	532
Tableau 62 – Champs du paramètre certificate_version	532
Tableau 63 – Valeurs autorisées pour ri_certificate_counter	533
Tableau 64 – Valeurs autorisées pour oosp_response_counter	534
Tableau 65 – Valeurs des indicateurs qui signalent l'absence de données/la présence de données	534
Tableau 66 – Valeurs autorisées pour subscriber_group_key_flag	535
Tableau 67 – Valeurs et signification de signature_type_flag	535
Tableau 68 – Syntaxe du message	541
Tableau 69 – Champs du message	543
Tableau 70 – Valeurs du paramètre status	544
Tableau 71 – Champs du paramètre certificate_version	544
Tableau 72 – Syntaxe du message	546
Tableau 73 – Champs du message	547
Tableau 74 – Valeurs du paramètre status	547
Tableau 75 – Syntaxe du message	548
Tableau 76 – Champs du message	549
Tableau 77 – Valeurs du paramètre status	550
Tableau 78 – Champs du paramètre certificate_version	550
Tableau 79 – Syntaxe du message	551
Tableau 80 – Format de l'objet contact	552
Tableau 81 – Contact_type	553
Tableau 82 – Règles de codage des données de contact	554
Tableau 83 – Protocoles hors ligne (du dispositif au RI)	555
Tableau 84 – Protocoles à 1 passe (du RI au dispositif)	555
Tableau 85 – Interrelation des protocoles	555
Tableau 86 – Champs du message	556
Tableau 87 – Valeurs du paramètre status	557
Tableau 88 – Champs du paramètre certificate_version	557

Tableau 89 – Syntaxe du message	562
Tableau 90 – Champs du message	564
Tableau 91 – Valeurs du paramètre status	564
Tableau 92 – Champs du paramètre certificate_version	565
Tableau 93 – Syntaxe du message	567
Tableau 94 – Syntaxe du message	569
Tableau 95 – Protocoles hors ligne (du dispositif au RI).....	570
Tableau 96 – Protocoles à 1 passe (du RI au dispositif).....	570
Tableau 97 – Interrelation des protocoles	570
Tableau 98 – Champs du message token_delivery_response	571
Tableau 99 – Address_mode pour le message token_delivery_response	572
Tableau 100 – Codes d'erreur.....	573
Tableau 101 – Mappage de address_mode pour les clés dans le message de réponse de distribution de jetons.....	575
Tableau 102 – Mappage de address_mode pour les clés dans le message de réponse de distribution de jetons.....	575
Tableau 103 – Syntaxe du message de réponse de distribution de jetons	576
Tableau 104 – Exigences pour la prise en charge de services et de flux de RI par les dispositifs IPDC sur DVB-H.....	581
Tableau 105 – Exigences pour la prise en charge de services et de flux d'émetteurs de droits par les fournisseurs de services dans les systèmes IPDC sur DVB-H.....	581
Tableau 106 – Définition des attributs SOC obligatoires dans les messages de requête/réponse.....	609
Tableau 107 – Occurrence des codes d'erreur dans les messages de réponse	611
Tableau 108 – Données à fournir au centre d'exploitation client.....	630
Tableau 109 – Options de la couche trafic pour la transmission en IPDC sur DVB-H	636
Tableau 110 – Format du flux d'émetteur de droits.....	641
Tableau 111 – Options de la couche trafic pour la transmission sur les réseaux MPEG2 TS.....	647
Tableau 112 – Table du KSM.....	648
Tableau 113 – Table des BCRO.....	649
Tableau 114 – Transport de messages de couche inscription à travers les sections MPEG dans les systèmes T/C/S	651
Tableau 115 – Syntaxe de la table de message d'inscription (RMT).....	652
Tableau 116 – Table de canal d'achat.....	664
Tableau 117 – Table de regroupement de services	668
Tableau 118 – Table d'élément d'achat.....	671
Tableau 119 – Balises du descripteur privé utilisées pour 18Crypt.....	672
Tableau 120 – Emplacements possibles des descripteurs.....	673
Tableau 121 – Service_ID_descriptor	673
Tableau 122 – Descripteur d'ID d'émetteur de droits.....	674
Tableau 123 – Descripteur d'emplacement d'informations d'achat.....	675
Tableau 124 – Descripteur d'élément d'achat.....	677
Tableau 125 – Valeurs de subscription_type.....	678
Tableau 126 – Exemple de prix selon différentes valeurs de l'emplacement du signe décimal.....	679

Tableau 127 – Descripteur de nom de fournisseur	680
Tableau 128 – Descripteur d'adressage Eurocrypt	680
Tableau 129 – Address_mode	681
Tableau 130 – Descripteur d'URL d'info	682
Tableau 131 – Descripteur d'URL de clé	682
Tableau 132 – Descripteur de liaison	683
Tableau 133 – Codage du type de liaison	684
Tableau 134 – Descripteur de liaison IP	684
Tableau 135 – ID définis par l'utilisateur	686
Tableau 136 – Ajouts à l'enregistrement de découverte de diffusion	690
Tableau 137 – Ajouts à l'enregistrement de découverte de contenu à la demande	690
Tableau 138 – Séquence d'événements pour l'achat et la distribution d'un élément de contenu à la demande	693
Tableau 139 – Options de la couche trafic pour la transmission sur les réseaux IP non fondés sur TS MPEG2	695
Tableau A.1 – Codes de statut/d'erreur	699
Tableau A.2 – Codage du décalage d'heure locale	703
Tableau A.3 – Jeu de clés normalisé avec un bloc RSA de taille 1024	705
Tableau A.4 – Jeu de clés normalisé avec un bloc RSA d'une autre taille	705
Tableau A.5 – Jeu de clés étendu avec un bloc RSA de taille 1024	706
Tableau A.6 – Jeu de clés étendu avec un bloc RSA d'une autre taille	706
Tableau A.7 – Probabilité d'erreur humaine de communication	715
Tableau A.8 – Valeurs de balise définies	719
Tableau A.9 – Valeurs de longueur définies	721
Tableau A.10 – Usage correct des valeurs de longueur	721
Tableau A.11 – Syntaxe du descripteur TAA	722
Tableau A.12 – Valeurs de l'algorithme TAA	723
Tableau A.13 – Présentation de message_tag	723
Tableau A.14 – Présentation des ID de tables	724
Tableau A.15 – Structure du texte multilingue	725
Tableau A.16 – Mappage des données de guide de service exigées pour l'ESG de la diffusion IPDC	736
Tableau A.17 – Mappage des données exigées du guide de service pour les tables PSI/SI DVB	738
Tableau A.18 – Mappage des données exigées du guide de service pour la TV anytime IPI BCG	742
Tableau A.19 – Élément permission mis à jour	755
Tableau A.20 – Élément d'accès	756
Tableau A.21 – Sémantique de l'élément <save>	758
Tableau A.22 – Utilisation des clés de programme et de service	759
Tableau A.23 – Champs de la zone GroupID	759
Tableau A.24 – Champs de la zone CommonHeaders	760
Tableau A.25 – Table de conformité pour IPDC sur DVB-H	774
Tableau A.26 – Table de conformité pour les systèmes DVB-T/C/S	778
Tableau A.27 – Table de conformité pour les systèmes IPTV	781

Tableau B.1 – Messages impliqués dans les systèmes EIC-T/C/S	810
Tableau B.2 – Informations de référence	814
Tableau B.3 – Exemple 1: CGF avec villes et régions	828
Tableau B.4 – Exemple 2: CGF avec sports et régions (indépendants)	828
Tableau B.5 – Exemple 3: CGF avec sports et régions (se chevauchant).....	830
Tableau B.6 – Catégories de références	837

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

ACCÈS AUX SERVICES FONDÉ SUR LE PROTOCOLE INTERNET (IP) ET SUR LE FLUX DE TRANSPORT (TS)

AVANT-PROPOS

- 1) La Commission Electrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
- 2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
- 3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
- 4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
- 5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
- 6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
- 7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
- 8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
- 9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

La Norme internationale IEC 62455 a été établie par le domaine technique 1: Terminaux pour les contenus audio, vidéo et services de données, du comité d'études 100 de l'IEC: Systèmes et équipements audio, vidéo et services de données.

Cette seconde édition annule et remplace la première édition publiée en 2007, dont elle constitue une révision technique.

Les principales modifications par rapport à l'édition précédente sont les suivantes:

- les développements récents des normes DVB et OMA ont entraîné certaines incompatibilités, résolues dans la seconde édition;
- des erreurs techniques ont été corrigées et des détails manquants ont été ajoutés;
- les références ont été mises à jour aux références disponibles les plus récentes;

- un certain nombre de corrections rédactionnelles et d'améliorations de lisibilité ont également été apportées, lorsque le texte original pouvait conduire à une mauvaise compréhension du fait de formulations peu claires ou de l'utilisation de plusieurs formes orthographiques pour un même élément.

La présente version bilingue (2021-12) correspond à la version anglaise monolingue publiée en 2010-12.

La version française de cette norme n'a pas été soumise au vote.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

ACCÈS AUX SERVICES FONDÉ SUR LE PROTOCOLE INTERNET (IP) ET SUR LE FLUX DE TRANSPORT (TS)

1 Domaine d'application

La présente Norme internationale spécifie le terminal d'un système d'achat et de protection de services pour diffusions numériques, appelé le système 18Crypt. Il s'applique dans l'ensemble des pays et régions qui comportent des systèmes de distribution de diffusion et multimédia conformes. Les lignes directrices pour des services de diffusion compatibles sont données dans la présente norme. Les fonctions d'achat et de protection de services fonctionnent dans un environnement de diffusion pure qui peut être combiné à un canal d'interactivité bidirectionnel.

La présente norme s'applique aux systèmes de diffusion suivants.

a) Systèmes de diffusion de données IP sur DVB-H

La diffusion de données IP sur DVB-H est un système de diffusion de bout en bout pour la distribution de tout type de contenu et de services numériques au moyen de mécanismes fondés sur IP optimisés pour les dispositifs avec des limitations sur les ressources de calcul et la batterie. Un aspect inhérent au système de diffusion de données IP est qu'il comprend un chemin de diffusion DVB unidirectionnel qui peut être combiné avec un chemin d'interactivité bidirectionnel mobile/cellulaire. La diffusion de données IP est donc une plateforme qui peut être utilisée pour permettre la convergence de services de diffusion/multimédia et de domaines de télécommunications (par exemple, mobile/cellulaire). La présente norme fixe les spécifications applicables à l'achat et à la protection de services de diffusion de données IP sur DVB-H (voir Tableau B.6 pour une présentation des références à un tel système).

b) Systèmes DVB T/C/S

Les systèmes DVB T/C/S sont des systèmes de diffusion de bout en bout pour les données audio/vidéo qui emploient un flux de transport MPEG2 et utilisent des réseaux de diffusion terrestres, par câble ou par satellite. La présente norme spécifie un système pour la protection de ces diffusions dans un environnement de diffusion pure. De plus, la présente norme spécifie comment effectuer l'achat, la gestion des clés et l'inscription sur un canal d'interactivité facultatif. Les technologies de protection offertes par la présente norme sont conçues pour fonctionner dans un environnement SimulCrypt DVB existant (voir Tableau B.6 pour une présentation des références).

c) Systèmes IP fondés sur TS MPEG2

Les systèmes IP fondés sur TS MPEG2 emploient des réseaux IP bidirectionnels pour la transmission (diffusion) de flux de transport MPEG2. La présente norme spécifie un système pour l'achat et la protection de services et de contenus livrés sur ces réseaux. La présente norme est par exemple applicable aux systèmes DVB-IP (voir Tableau B.6 pour une présentation des références).

d) Systèmes IP non fondés sur TS MPEG2

Les systèmes IP non fondés sur TS MPEG2 emploient des réseaux IP bidirectionnels pour la distribution (diffusion) de données audio/vidéo ou autres au moyen de protocoles IP plutôt que de flux de transport MPEG2. La présente norme spécifie un système destiné à l'achat et à la protection de services et de contenus livrés sur ces réseaux (voir Tableau B.6 pour une présentation des références).

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/IEC 8859-1:1998, *Information technology – 8-bit single-byte coded graphic character sets – Part 1: Latin alphabet No. 1* (disponible en anglais seulement)

ISO/IEC 13818-1:2007, *Information technology – Generic coding of moving pictures and associated audio information: Systems* (disponible en anglais seulement)

ISO/IEC 14496-12:2008, *Information technology – Coding of audio-visual objects – Part 12: ISO base media file format* (disponible en anglais seulement)

ISO/IEC 15938-5:2003, *Information technology – Multimedia content description interface – Part 5: Multimedia description schemes* (disponible en anglais seulement)

ISO 639-1:2002, *Codes pour la représentation des noms de langue – Partie 1: Code Alpha-2*

ISO 639-2:1998, *Codes pour la représentation des noms de langue – Partie 2: Code Alpha-3*

ISO 3166 (toutes les parties), *Codes pour la représentation des noms de pays et de leurs subdivisions*

ISO 4217, *Codes pour la représentation des monnaies et types de fonds*

ISO 8601:2004, *Éléments de données et formats d'échange – Echange d'information – Représentation de la date et de l'heure*

ETSI EN 102 034, *Digital Video Broadcasting (DVB) – Transport of MPEG-2-based DVB services over I- based networks* (disponible en anglais seulement)

ETSI EN 300 468, *Digital Video Broadcasting (DVB) – Specification for Service Information (SI) in DVB systems* (disponible en anglais seulement)

ETSI EN 301 192, *Digital Video Broadcasting (DVB) – DVB specification for data broadcasting* (disponible en anglais seulement)

ETSI EN 302 304, *Digital Video Broadcasting (DVB) – Transmission system for handheld terminals (DVB-H)* (disponible en anglais seulement)

ETSI TS 102 539, *Digital Video Broadcasting (DVB) – Carriage of broadband content guide (BCG) information over internet protocol (IP)* (disponible en anglais seulement)

ETSI ETR 162, http://www.dvb.org/products_registration/dvb_identifiers/ (ce site web remplace l'ETR 162)

ETSI ETR 289, *Digital Video Broadcasting (DVB) – Support for use of scrambling and conditional access (CA) within digital broadcasting systems* (disponible en anglais seulement)

ETSI TS 102 471, *Digital Video Broadcasting (DVB) – IP datacast over DVB-H: Electronic service guide (ESG)* (disponible en anglais seulement)

ETSI TS 102 472, *Digital Video Broadcasting (DVB) – IP datacast over DVB-H: Content delivery protocols* (disponible en anglais seulement)

ETSI TS 102 822-3-1, *Broadcast and on-line services: Search, select, and rightful use of content on personal storage systems (TV-anytime) – Part 3: Metadata – Sub-part 1: Phase 1 – Metadata schemas* (disponible en anglais seulement)

ETSI TS 103 197, *Digital Video Broadcasting (DVB) – SimulCrypt Head-end implementation of DVB SimulCrypt, v1.4.1* (disponible en anglais seulement)