

# INTERNATIONAL STANDARD

# IEC 62455

First edition  
2007-06

---

---

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



Commission Electrotechnique Internationale  
International Electrotechnical Commission  
Международная Электротехническая Комиссия

PRICE CODE **XP**

*For price, see current catalogue*

## CONTENTS

FOREWORD.....	13
1 Scope.....	15
2 Normative references .....	15
3 Terms, definitions and abbreviations .....	17
3.1 Terms and definitions .....	17
3.2 Symbols .....	22
3.3 Abbreviations .....	23
3.4 Identifiers assigned by external entities .....	27
4 General .....	27
4.1 General description of the system and elements.....	28
4.1.1 Selected technologies .....	28
4.1.2 Overview of four-layer model for service protection .....	30
4.2 End-to-end system .....	32
4.3 Supported systems and device types.....	32
4.4 Service protection versus content protection .....	34
5 General specifications .....	35
5.1 End-to-end architecture .....	35
5.2 Special cases .....	37
5.2.1 Free-to-air services .....	37
5.2.2 Free-to-view services .....	37
5.3 Service guide and purchase .....	37
5.4 Four-layer model – Key hierarchy.....	38
5.4.1 Keys on the traffic layer.....	39
5.4.2 Keys on the key stream layer.....	39
5.4.3 Keys on the rights management layer (interactive mode) .....	41
5.4.4 Keys on the rights management layer (broadcast mode).....	42
5.4.5 Keys on the registration layer (interactive mode) .....	42
5.4.6 Keys on the registration layer (broadcast mode).....	42
5.4.7 Authentication overview.....	45
5.5 Deployment for broadcast mode of operation.....	46
5.5.1 Concept of Domains –Interactive and broadcast domains .....	46
5.5.2 Addressing (group/subset/device/domain) .....	47
5.5.3 Zero message broadcast encryption scheme .....	49
6 Traffic layer.....	51
6.1 IPsec.....	52
6.1.1 General .....	52
6.1.2 Selectors .....	53
6.1.3 Encapsulation protocol and mode .....	53
6.1.4 Encryption algorithm.....	54
6.1.5 Authentication algorithm .....	54
6.1.6 Security association management .....	54
6.2 ISMACryp.....	54
6.2.1 Streamed content .....	54
6.2.2 Downloadable audio/visual content (stored in MP4 files).....	55
6.2.3 Use of ISMACryp with the rights management and key stream layers .....	56

6.3	SRTP .....	56
6.3.1	Key management.....	58
6.3.2	Encryption algorithm.....	58
6.3.3	Authentication algorithm .....	59
6.4	MPEG2 TS crypt .....	59
6.4.1	General .....	59
6.4.2	Transport stream level scrambling .....	60
6.4.3	PES level scrambling.....	61
6.4.4	Descrambling MPEG2 content .....	61
6.4.5	Supported ciphers .....	62
6.4.6	Key management.....	63
7	Key stream layer .....	63
7.1	General.....	63
7.2	Format of the key stream message (KSM) .....	63
7.2.1	Descriptors for access_criteria_descriptor_loop.....	66
7.2.2	Constants .....	73
7.2.3	Coding and semantics of attributes .....	73
8	Rights management layer .....	81
8.1	General.....	81
8.1.1	Requirements for service ROs .....	82
8.1.2	Requirements for programme ROs.....	82
8.2	Format of rights objects.....	83
8.2.1	Format of an Interactivity channel rights object (ICRO).....	83
8.2.2	Format of a broadcast rights object (BCRO) .....	83
9	Registration layer .....	98
9.1	RI context.....	98
9.2	Registration layer protocols and message specification .....	99
9.2.1	Interactivity channel registration layer specification .....	99
9.2.2	Broadcast channel registration layer specification .....	99
9.2.3	Domain joining and leaving.....	134
9.2.4	Token handling .....	149
9.2.5	Mixed-mode registration for interactive and broadcast modes of operation .....	156
10	Signalling and service guide .....	157
10.1	Signalling requirements .....	157
10.1.1	Requirements for signalling the KSM .....	158
10.1.2	Requirements for signalling of services .....	158
10.2	Service guide requirements .....	158
10.3	Service guide recommendations .....	158
11	Rights issuer services and rights issuer streams .....	159
11.1	General.....	159
11.1.1	Requirements for rights issuer services in IPDC over DVB-H systems .....	159
11.1.2	Requirements for rights issuer services in DVB-T/C/S systems.....	159
11.1.3	Requirements for the support of rights issuer services and streams in IPTV systems .....	160
11.2	Usage of rights issuer streams and services.....	160
11.2.1	Scheduled RI stream .....	161
11.2.2	<i>Ad hoc</i> RI stream.....	161
11.2.3	In-band RI streams within a media service.....	161

12	Service subscription and purchase .....	162
12.1	Purchase over an interactivity channel .....	163
12.1.1	Typical purchase sequences.....	164
12.1.2	Protocol.....	187
12.1.3	XML schemas for request and response messages .....	187
12.1.4	XML schema definition for request and response related XML elements .....	202
12.2	Purchase for mixed-mode devices.....	207
12.3	Out-of-band purchase.....	207
12.3.1	Means of purchase – Introduction.....	207
12.3.2	Out-of-band purchase from service guide data .....	208
12.4	Required service guide Information .....	209
12.4.1	Service operation centre (including service distribution management) .....	210
12.4.2	Customer operation centre (including service subscription management) .....	210
12.4.3	Service.....	211
12.4.4	ScheduleItem .....	212
12.4.5	ContentItem.....	212
12.4.6	Purchase item .....	213
12.4.7	Purchase data .....	213
13	Protection of IPDC over DVB-H systems.....	213
13.1	Delivery of traffic layer data in IPDC over DVB-H systems.....	214
13.2	Delivery of key stream data in IPDC over DVB-H systems .....	214
13.3	Delivery of rights management data in IPDC over DVB-H systems .....	214
13.3.1	Delivery of ICROs in IPDC over DVB-H systems over interactivity channel .....	214
13.3.2	Delivery of BCROs in IPDC over DVB-H systems over broadcast channel .....	214
13.4	Delivery of registration data in IPDC over DVB-H systems.....	214
13.4.1	Delivery of registration data in IPDC over DVB-H systems over an interactivity channel.....	214
13.4.2	Delivery of registration data in IPDC over DVB-H systems over a broadcast channel .....	215
13.5	Signalling and service guides in IPDC over DVB-H systems .....	215
13.5.1	Signalling of KSM in IPDC over DVB-H systems .....	215
13.5.2	The service guide for IPDC over DVB-H systems.....	215
13.6	Format and use of RI streams over IPDC over DVB-H systems .....	216
13.6.1	IP characteristics.....	216
13.6.2	RI stream packet format .....	217
13.6.3	Implementation notes .....	218
13.6.4	Mapping of messages to RI services and streams .....	219
13.6.5	Discovery of RI services, streams and schedule Information .....	220
13.6.6	Certificate chain updates.....	220
13.6.7	Resending of BCROs .....	221
13.6.8	Summary of requirements for rights issuers.....	222
13.6.9	Summary of requirements for devices.....	222
13.6.10	Mapping of messages to DVB-H time sliced bursts.....	223
14	Protection of DVB T/C/S systems .....	223
14.1	Delivery of traffic layer data in DVB T/C/S systems .....	223
14.2	Delivery of key stream data in DVB T/C/S systems.....	224

14.3	Delivery of rights management data in DVB T/C/S systems .....	224
14.3.1	Delivery of ICROs in DVB T/C/S systems over interactivity channel .....	225
14.3.2	Delivery of BCROs in DVB T/C/S systems over broadcast channel.....	225
14.4	Delivery of registration data in DVB T/C/S systems .....	226
14.4.1	Delivery of registration data in DVB T/C/S systems over an interactivity channel .....	226
14.4.2	Delivery of registration data in DVB T/C/S systems over a broadcast channel .....	226
14.4.3	Registration message table .....	227
14.5	Signalling and service guide in DVB T/C/S systems .....	228
14.5.1	Signalling of encrypted services in DVB T/C/S systems.....	229
14.5.2	SI tables .....	237
14.5.3	SI descriptors .....	246
14.6	User-defined identifiers used in DVB-SI tables .....	260
14.7	Scope of identifiers used in DVB-SI tables .....	260
14.8	Format of RI services over DVB-T/C/S systems.....	261
14.8.1	RI stream packet format .....	261
14.8.2	Addressing of objects .....	261
14.8.3	Mapping of messages to RI services and streams .....	261
15	Protection of MPEG2 TS-based IP systems .....	261
15.1	Encapsulation of an MPEG2 TS in IP .....	262
15.2	Delivery of traffic layer data in MPEG2 TS-based IP systems .....	262
15.3	Delivery of key stream data in MPEG2 TS-based IP systems .....	262
15.4	Delivery of rights management data in MPEG2 TS-based IP systems.....	262
15.5	Delivery of registration data in MPEG2 TS-based IP systems .....	262
15.6	Signalling and service guides in MPEG2 TS-based IP systems .....	262
15.6.1	Signalling and the service guide in DVB-IPI systems .....	262
15.6.2	Signalling and service guides in non-DVB-IPI systems .....	265
15.7	Format of RI services over MPEG2 TS-based IP systems.....	265
15.8	Content-on-demand support .....	265
15.8.1	General .....	265
15.8.2	Content-on-demand trick play support .....	266
15.9	Use of server-side purchase interfaces.....	266
15.9.1	Example showing registration via a web interface.....	267
15.9.2	Example showing purchase via a web interface .....	267
16	Protection of non-MPEG2 TS-based IP systems .....	267
16.1	Delivery of traffic layer data in non-MPEG2 TS-based IP systems .....	267
16.2	Delivery of key stream data in non-MPEG2 TS-based IP systems.....	268
16.3	Delivery of rights management data in non-MPEG2 TS-based IP systems.....	268
16.4	Delivery of registration data in non-MPEG2 TS-based IP systems .....	268
16.5	Signalling and service guides in non-MPEG2 TS-based IP systems.....	268
16.6	Format of RI services over non-MPEG2 TS-based IP systems .....	268
16.7	Content-on-demand support .....	268
	Annex A (normative) .....	269
	Annex B (informative) .....	350
	Bibliography.....	401

Figure 1 – System overview .....	28
Figure 2 – Service protection via four-layer model .....	30
Figure 3 – Highly simplified view of the end-to-end system .....	32
Figure 4 – Service protection versus content protection .....	34
Figure 5 – Service protection and purchase entities and names (broadcast rchitecture) .....	35
Figure 6 – Public key infrastructure.....	36
Figure 7 – Overview of service guide and purchase .....	38
Figure 8 – 4-layer key hierarchy – Use of SEK only .....	40
Figure 9 – 4-layer key hierarchy – Use of PEK and SEK .....	41
Figure 10 – Authentication hierarchy.....	45
Figure 11 – Explaining the concept of addressing .....	47
Figure 12 – (Oversimplified) group BCRO .....	48
Figure 13 – (Oversimplified) subscriber group BCRO .....	48
Figure 14 – (Oversimplified) unique device BCRO .....	49
Figure 15 – (Oversimplified) broadcast domain BCRO .....	49
Figure 16 – Example of a zero message tree with 3 nodes (keys) .....	50
Figure 17 – IPsec security association elements .....	53
Figure 18 – ISMACryp key management .....	56
Figure 19 – SRTP cryptographic context management.....	57
Figure 20 – MPEG2 transport stream cryptographic context management.....	59
Figure 21 – Single-key versus dual-key TS over time.....	62
Figure 22 – Registration for broadcast mode of operation with one ROT .....	99
Figure 23 – Offline NDD protocol .....	101
Figure 24 – Samples of notification displays .....	101
Figure 25 – Offline NSD protocol .....	102
Figure 26 – Action request code (ARC).....	102
Figure 27 – Samples of notification displays showing an ARC message.....	103
Figure 28 – Sample of token consumption reporting notification display.....	104
Figure 29 – Sample of TAA report display.....	106
Figure 30 – 1-pass PDR protocol – (First) device registration .....	106
Figure 31 – 1-pass IRD protocol – RI initiated message to device (here re-registration). .....	107
Figure 32 – Unique device number .....	109
Figure 33 – Device_registration_response() message.....	120
Figure 34 – Structure of device_registration_response() message. ....	121
Figure 35 – Domain_registration_response() message.....	140
Figure 36 – Structure of domain_registration_response() message.....	141
Figure 37 – Registration for mixed-mode operation with one ROT.....	157
Figure 38 – Relationship between RI service and RI streams, and other services and RI streams .....	160
Figure 39 – Message flows for service subscription and purchase for the connected mode of operation.....	162
Figure 40 – Message flows for service subscription and purchase for the unconnected mode of operation.....	163

Figure 41 – Interactions for bulk download of service and programme keys .....	165
Figure 42 – Interactions for bulk download of purchase information .....	166
Figure 43 – Interactions for announcement of purchase items in service guide .....	167
Figure 44 – Interactions for pricing inquiry .....	169
Figure 45 – Interactions for unsuccessful purchase.....	173
Figure 46 – Interactions for successful purchase .....	177
Figure 47 – Interactions for subscription RO renewal and asynchronous charging .....	182
Figure 48 – Interactions for asynchronous charging and cancellation of open-ended subscriptions .....	183
Figure 49 – Interactions for acquisition and charging of tokens .....	186
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.....	209
Figure 52 – Example mapping of objects to RI stream packets.....	217
Figure 53 – Signalling of encrypted services and their associated key streams .....	230
Figure 54 – Signalling of encrypted services in the SDT.....	231
Figure 55 – Signalling of the rights issuer service in the SDT.....	232
Figure 56 – Addressing of a rights issuer service .....	232
Figure 57 – Signalling of purchase information via the SDT .....	233
Figure 58 – Signalling of purchase information via the CA_descriptor in the CAT.....	234
Figure 59 – Signalling of purchase information via the private data block of the CA_descriptor in the CAT .....	235
Figure 60 – Relationship between PCT, PIT, SBT and SDT .....	236
Figure 61 – Alternative usage of the purchase_item_descriptor in the SDT and EIT .....	237
Figure A.1 – Sample notification display .....	270
Figure A.2 – Conversion routes between modified Julian date (MJD) and coordinated universal time (UTC).....	273
Figure A.3 – Node numbering .....	278
Figure A.4 – AES for key derivation .....	279
Figure A.5 – Sample tree with correct node and device numbering. ....	281
Figure A.6 – Computation of the TAA_report_code .....	286
Figure A.7 – Node numbering .....	291
Figure A.8 – Computation of the report_authentication_code .....	297
Figure A.9 – Relationship between DVB-T/C/S PSI/SI tables .....	309
Figure A.10 – Relationships between the defined types .....	311
Figure A.11 – XML fragment for SOC identifier .....	313
Figure A.12 – XML fragment for service base CID.....	313
Figure A.13 – Definition of UniversalPurchaseItemType .....	314
Figure A.14 – Definition of the ServiceBundleType .....	314
Figure A.15 – Definition of UniversalServiceInformationType .....	315
Figure A.16 – Definition of UniversalOnDemandServiceType .....	315
Figure A.17 – Definition of UniversalPurchaseType.....	315
Figure A.18 – Recording and super-distributing the recorded asset.....	325
Figure A.19 – Format of the OMADRMRecordingTimestamp.....	328

Figure A.20 – Format of the OMADRMRecordingInformationBlock .....	329
Figure A.21 – 18Crypt namespace declaration .....	330
Figure B.1 – Rights Issuer communication with various types of devices in IPDC over DVB-H systems.....	352
Figure B.2 – Rights Issuer communication with various types of devices in DVB-T/C/S systems .....	355
Figure B.3 – Rights Issuer communication with various types of devices in IP systems .....	357
Figure B.4 – Purchase steps in case of an Interactive device .....	358
Figure B.5 – Purchase steps in case of a broadcast device.....	360
Figure B.6 – Consumption steps from the broadcaster point of view.....	362
Figure B.7 – Consumption steps from the device point of view .....	363
Figure B.8 – Function blocks of service protection head-end.....	372
Figure B.9 – Systems and network elements of service protection head-end.....	373
Figure B.10 – IEC T/C/S components integrated into DVB SimulCrypt head-end.....	375
Figure B.11 – Locating 18Crypt KSM & BCRO as well as EMM & ECM .....	377
Figure B.12 – Carrying messages over the network .....	378
Figure B.13 – Sample network set-ups using the location descriptors .....	379
Figure B.14 – Expanding the IEC T/C/S head-end components.....	379
Figure B.15 – Deployment option A (combining DIST Mgmt and RI in SOC) – Local scenario.....	384
Figure B.16 – Deployment option A (combining DIST Mgmt and RI in SOC) – Roaming scenario.....	386
Figure B.17 – Deployment option B (combining SUB Mgmt and RI in COC) – Local scenario.....	388
Figure B.18 – Deployment option B (combining SUB Mgmt and RI in COC) – Roaming scenario.....	389
Figure B.19 – Scenarios 1 and 2 for bosb_masks .....	393
Figure B.20 – Scenarios 3 and 4 for bosb_masks .....	395
Figure B.21 – Scenarios 5 and 6 for bosb_masks .....	396
Figure B.22 – Scenarios 7 and 8 for bosb_masks .....	397
Figure B.23 – Scenarios 9 and 10 for bosb_masks (precedence).....	398
Table 1 – Supported systems and device types .....	33
Table 2 – Keypset in the registration data .....	42
Table 3 – Definition of transport_scrambling_control bits .....	60
Table 4 – Definition of pes_scrambling_control field bits.....	61
Table 5 – Descrambling possibility matrix .....	62
Table 6 – Supported ciphers for MPEG2 TS crypt .....	62
Table 7 – Format of key stream message .....	64
Table 8 – Descriptors for access_criteria_descriptor_loop .....	66
Table 9 – Access_criteria_descriptors.....	66
Table 10 – Parental_rating access criteria descriptor.....	66
Table 11 – Parental rating values for each parental rating type.....	67
Table 12 – Copy_control_information access criteria descriptor.....	68
Table 13 – Bit assignments of copy_control_information_byte .....	68



Table 14 – CCI bit assignments .....	69
Table 15 – EMI values and content .....	69
Table 16 – APS value definitions .....	69
Table 17 – CIT values and application .....	70
Table 18 – RCT values and application .....	70
Table 19 – Blackout_spotbeam access criteria descriptor .....	71
Table 20 – Operator field values and their meaning .....	71
Table 21 – Constants in key stream message .....	73
Table 22 – Content_key_index options .....	75
Table 23 – cipher_mode options .....	76
Table 24 – Obtaining the content key .....	77
Table 25 – Traffic key lifetime .....	78
Table 26 – Values of permissions_category and their meaning .....	79
Table 27 – Format of BCRO .....	83
Table 28 – Address_mode .....	85
Table 29 – Asset format .....	87
Table 30 – Asset_type .....	88
Table 31 – Mapping of address_mode to keys .....	88
Table 32 – Mapping of address_mode to keys .....	89
Table 33 – Mapping of address_mode to keys .....	89
Table 34 – Permission format .....	90
Table 35 – Action format .....	91
Table 36 – Action_type .....	91
Table 37 – Constraint format .....	92
Table 38 – Format of constraint_descriptor .....	92
Table 39 – Constraint_tag .....	93
Table 40 – Format of count_constraint_descriptor .....	93
Table 41 – Format of timed_count_constraint_descriptor .....	93
Table 42 – Format of datetime_constraint_descriptor .....	94
Table 43 – Format of interval_constraint_descriptor .....	95
Table 44 – Format of accumulated_constraint_descriptor .....	95
Table 45 – Format of individual_constraint_descriptor .....	96
Table 46 – Id_type .....	96
Table 47 – Format of system_constraint_descriptor .....	96
Table 48 – Format of metering_constraint_descriptor .....	97
Table 49 – Registration types .....	98
Table 50 – NSD action request code fields .....	102
Table 51 – NSD action types .....	103
Table 52 – Token consumption data .....	104
Table 53 – TAA report data .....	106
Table 54 – Messages of the 1-pass IRD protocol .....	107
Table 55 – UDN explanation .....	110
Table 56 – Major industry identifier .....	110

Table 57 – longform_udn .....	111
Table 58 – Notify device data message parameters .....	111
Table 59 – Device data .....	112
Table 60 – Message fields .....	113
Table 61 – Status values .....	114
Table 62 – Fields of certificate_version parameter .....	114
Table 63 – Allowed values for ri_certificate_counter .....	115
Table 64 – Allowed values for ocsp_response_counter .....	116
Table 65 – Values for flags signalling data absent / data present .....	116
Table 66 – Allowed values for subscriber_group_key_flag .....	117
Table 67 – Values and their meaning for signature_type_flag .....	117
Table 68 – Message syntax .....	122
Table 69 – Message fields .....	124
Table 70 – Status values .....	125
Table 71 – Fields of certificate_version parameter .....	125
Table 72 – Message syntax .....	127
Table 73 – Message fields .....	128
Table 74 – Status values .....	128
Table 75 – Message syntax .....	129
Table 76 – Message fields .....	130
Table 77 – Status values .....	130
Table 78 – Fields of certificate_version parameter .....	131
Table 79 – Message syntax .....	132
Table 80 – Format of contact object .....	133
Table 81 – Contact_type .....	133
Table 82 – Encoding rules for contactdata .....	134
Table 83 – Offline protocols (from device to RI) .....	135
Table 84 – 1-pass protocols (from RI to device) .....	135
Table 85 – Protocol interrelation .....	135
Table 86 – Message fields .....	136
Table 87 – Status values .....	137
Table 88 – Fields of certificate_version parameter .....	137
Table 89 – Message syntax .....	142
Table 90 – Message fields .....	143
Table 91 – Status values .....	144
Table 92 – Fields of certificate_version parameter .....	144
Table 93 – Message syntax .....	146
Table 94 – Message syntax .....	148
Table 95 – Offline protocols (from device to RI) .....	149
Table 96 – 1-pass protocols (from RI to device) .....	149
Table 97 – Protocol interrelation .....	149
Table 98 – Fields of token delivery response message .....	150
Table 99 – Address_mode for token delivery response message .....	151

Table 100 – Message error codes .....	152
Table 101 – Mapping of address_mode to keys for the token delivery response message .....	153
Table 102 – Mapping of address_mode to keys for the token delivery response message .....	154
Table 103 – Syntax of token delivery response message .....	154
Table 104 – Requirements for the support of RI services and streams by IPDC over DVB-H Devices .....	159
Table 105 – Requirements for the support of RI services and streams by service providers in IPDC over DVB-H systems .....	159
Table 106 – Definition of mandatory SOC attributes in request/response messages .....	190
Table 107 – Occurrence of error codes in response messages .....	191
Table 108 – Data to be provided to the customer operation centre .....	208
Table 109 – Traffic layer options for transmission over IPDC over DVB-H .....	214
Table 110 – Format of the RI stream .....	218
Table 111 – Traffic layer options for transmission over MPEG2 TS-based networks .....	223
Table 112 – KSM table .....	224
Table 113 – BCRO table .....	225
Table 114 – Carrying registration layer messages via MPEG sections in T/C/S system .....	226
Table 115 – Syntax of registration message table (RMT) .....	227
Table 116 – Purchase channel table .....	238
Table 117 – Service bundle table .....	242
Table 118 – Purchase item table .....	245
Table 119 – Private descriptor tags used for 18Crypt .....	246
Table 120 – Possible locations of descriptors .....	247
Table 121 – Service_ID_descriptor .....	247
Table 122 – Right Issuer ID descriptor .....	248
Table 123 – Purchase info location descriptor .....	249
Table 124 – Purchase item descriptor .....	250
Table 125 – Subscription_type values .....	252
Table 126 – Example price with different decimal point location values .....	253
Table 127 – Provider name descriptor .....	254
Table 128 – Eurocrypt addressing descriptor .....	254
Table 129 – Address_mode .....	255
Table 130 – Info URL descriptor .....	256
Table 131 – Key URL descriptor .....	256
Table 132 – Linkage descriptor .....	257
Table 133 – Linkage type coding .....	258
Table 134 – IP linkage descriptor .....	258
Table 135 – User defined IDs .....	260
Table 136 – Additions to the broadcast discovery record .....	263
Table 137 – Additions to the content-ondemand discovery record .....	263
Table 138 – Sequence of events for purchase and supply of a content-on-emand item .....	266
Table 139 – Traffic lyer options for transmission over non-MPEG2 TS-ased IP networks .....	267

Table A.1 – Status/error codes .....	271
Table A.2 – Local time offset coding .....	275
Table A.3 – Standard keyset with RSA block size 1024.....	276
Table A.4 – Standard keyset with other RSA block sizes.....	277
Table A.5 – Extended keyset with RSA block size 1024 .....	277
Table A.6 – Extended keyset with other RSA block sizes .....	278
Table A.7 – Error likelihood in human communication .....	286
Table A.8 – Defined tag values .....	290
Table A.9 – Defined length values .....	292
Table A.10 – Correct usage of length values.....	292
Table A.11 – TAA descriptor syntax .....	294
Table A.12 – TAA algorithm values .....	294
Table A.13 – Message_tag overview.....	295
Table A.14 – Table ID overview .....	295
Table A.15 – Multilingual text structure .....	296
Table A.16 – Mapping of required service guide data to the IPDC ESG.....	306
Table A.17 – Mapping of required service guide data to DVB PSI/SI tables.....	308
Table A.18 – Mapping of required service guide data to IPI BCG/TV anytime.....	311
Table A.19 – Updated permission element.....	323
Table A.20 – Access element.....	324
Table A.21 – Semantics of the save element .....	326
Table A.22 – Use of programme and service keys.....	326
Table A.23 – Fields in the GroupID box.....	327
Table A.24 – CommonHeaders box fields .....	327
Table A.25 – Conformance table for IPDC over DVB-H systems .....	339
Table A.26 – Conformance table for DVB-T/C/S systems .....	343
Table A.27 – Conformance table for IPTV systems .....	346
Table B.1 – Messages involved in IEC T/C/S systems.....	374
Table B.2 – Reference overview information .....	378
Table B.3 – Example 1: CGF with cities and regions .....	392
Table B.4 – Example 2: CGF with sports and regions (independent) .....	392
Table B.5 – Example 3: CGF with sports and regions (overlapping) .....	394

## 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 provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
- 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, of IEC technical committee 100: Audio, video and multimedia systems and equipment.

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

CDV	Report on voting
100/1141A/CDV	100/1222/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 maintenance result 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.

A bilingual version of this publication may be issued at a later date.

## 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) IPDC 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 B.10.3 for an overview of references).

#### 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 B.10.2 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-IP1 systems (see B.10.4 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 B.10.4 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, *8-bit single-byte coded graphic character sets – Part 1: Latin alphabet No. 1*

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

ISO/IEC 14496-12:2005, *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/](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*