

This is a preview - click here to buy the full publication



IEC 62455

Edition 2.0 2010-12

INTERNATIONAL STANDARD



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

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE **XH**

ICS 33.170; 35.100; 35.240.99

ISBN 978-2-88912-289-9

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 | | 407 |
| 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 | 391 |
| Figure B.17 – Deployment option B (combining SUB Mgmt and RI in COC) – Local scenario | 393 |
| Figure B.18 – Deployment option B (combining SUB Mgmt and RI in COC) – Roaming scenario | 394 |
| Figure B.19 – Scenarios 1 and 2 for bosb_masks | 398 |
| Figure B.20 – Scenarios 3 and 4 for bosb_masks | 400 |
| Figure B.21 – Scenarios 5 and 6 for bosb_masks | 401 |
| Figure B.22 – Scenarios 7 and 8 for bosb_masks | 402 |
| Figure B.23 – Scenarios 9 and 10 for bosb_masks (precedence)..... | 403 |
| Figure B.24 – Diagram of keyset_block, sessionkey_block and surplus_block..... | 405 |
| | |
| 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 ocsp_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 | 397 |
| Table B.4 – Example 2: CGF with sports and regions (independent) | 397 |
| Table B.5 – Example 3: CGF with sports and regions (overlapping) | 399 |
| 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.

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

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*