# SLOVENSKI STANDARD
# SIST EN 62455:2011

**01-julij-2011**

---

**Dostop do storitve na podlagi internetnega protokola (IP) in transportne struje (TS) (IEC 62455:2010)**

Internet protocol (IP) and transport stream (TS) based service access (IEC 62455:2010)

Dienstzugang auf Basis von Internet- Protokoll (IP) und Transportstrom (TS) (IEC 62455:2010)



Accès aux services employant le protocole internet (IP) et le flux de transport (TS) (CEI 62455:2010)



**Ta slovenski standard je istoveten z:** **EN 62455:2011**

---

**ICS:**

| | | |
|---|---|---|
| 33.160.01 | Avdio, video in avdiovizualni sistemi na splošno | Audio, video and audiovisual systems in general |
| 35.100.01 | Medsebojno povezovanje odprtih sistemov na splošno | Open systems interconnection in general |

**SIST EN 62455:2011** **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

# EN 62455

February 2011

ICS 33.170; 35.100; 35.240.99

English version

# Internet protocol (IP) and transport stream (TS) based service access
(IEC 62455:2010)

Accès aux services employant le protocole internet (IP) et le flux de transport (TS)
(CEI 62455:2010)

Dienstzugang auf Basis von Internet-Protokoll (IP) und Transportstrom (TS)
(IEC 62455:2010)

This European Standard was approved by CENELEC on 2011-01-19. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.



Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the Central Secretariat or to any CENELEC member.



This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the Central Secretariat has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland and the United Kingdom.

CENELEC

European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

**Management Centre: Avenue Marnix 17, B - 1000 Brussels**



Ref. No. EN 62455:2011 E

## Foreword

The text of document 100/1551/CDV, future edition 2 of IEC 62455, prepared by IEC TC 100, Audio, video and multimedia systems and equipment, was submitted to the IEC-CENELEC parallel vote and was approved by CENELEC as EN 62455 on 2011-01-19.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN and CENELEC shall not be held responsible for identifying any or all such patent rights.

The following dates were fixed:

| | | |
|---|---|---|
| – latest date by which the EN has to be implemented at national level by publication of an identical national standard or by endorsement | (dop) | 2011-10-19 |
| – latest date by which the national standards conflicting with the EN have to be withdrawn | (dow) | 2014-01-19 |

Annex ZA has been added by CENELEC.

## Endorsement notice

The text of the International Standard IEC 62455:2010 was approved by CENELEC as a European Standard without any modification.

# Annex ZA
(normative)

## Normative references to international publications with their corresponding European publications

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.

NOTE When an international publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

| Publication | Year | Title | EN/HD | Year |
|---|---|---|---|---|
| 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 | Series | 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 | - | - |
| 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 | - | - |
| ETSI EN 301 192 | - | Digital Video Broadcasting (DVB) - DVB specification for data broadcasting, V1.2.1 | - | - |
| ETSI EN 302 304 | - | Digital Video Broadcasting (DVB); Transmission System for Handheld Terminals (DVB-H) | - | - |
| ETSI EN 300 468 | - | Digital Video Broadcasting (DVB): Specification for Service Information (SI) in DVB systems | - | - |
| ETSI TS 102 034 | - | Digital Video Broadcasting (DVB);Transport of MPEG-2 TS Based DVB Services over IP Based Networks | - | - |
| ETSI TS 102 539 | - | Digital Video Broadcasting (DVB);Carriage of Broadband Content Guide (BCG) information over Internet Protocol (IP) | - | - |

| Publication | Year | Title | EN/HD | Year |
|---|---|---|---|---|
| ETSI ETR 162 | - | Digital Video Broadcasting (DVB);Allocation of Service Information (SI) codes for DVB systems | - | - |
| 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 | - | - |
| TSI 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);Head-end implementation of DVB SimulCrypt | - | - |

# IEC 62455

Edition 2.0 2010-12

# INTERNATIONAL STANDARD

colour inside

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



INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE XP

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 *Ad hoc* 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