

INTERNATIONAL STANDARD

**IEC
62455**

First edition
2007-06

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

Withdrawn



Reference number
IEC 62455:2007(E)



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2007 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.

If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

IEC Central Office
3, rue de Varembe
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,...). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

INTERNATIONAL STANDARD

**IEC
62455**

First edition
2007-06

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

Withdrawn



Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE **XH**

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 architecture)	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	162

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 – Keyset 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	

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 ocsf_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.

Withdrawn

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-IPI 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/ (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*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1.1

18Crypt

service purchase and protection system specified by this standard

3.1.2

broadband content guide

service guide in DVB-IPI based IP systems; see ETSI EN 102 034

3.1.3

broadcast channel

broadcast network

NOTE See also other definitions using "broadcast".

3.1.4

broadcast device

device that is capable of receiving protected broadcasts but which cannot access an interactivity channel

NOTE All messages sent to such a device are delivered via a broadcast channel and all communications from the device to rights issuers is done out of band.

3.1.5

broadcast domain

group of devices for which rights objects granting the same rights to the whole group can be issued via a broadcast channel

3.1.6

broadcast network

digital transmission system supporting only unidirectional communication from the broadcaster to multiple devices

3.1.7

broadcast rights object

content, programme or service rights object delivered over the broadcast network

3.1.8

broadcast service

service carried over a broadcast network

3.1.9

broadcast

unidirectional distribution to all receivers

3.1.10

conditional access

encryption/decryption management method (security system) where the broadcaster controls the subscriber's access to digital services

3.1.11

content

any form of digital media that can be acquired and presented by a device

3.1.12

content on demand

delivery of content to a single device as a result of a specific request from a user

3.1.13

content protection

protection of content such that it can only be presented by authorized devices

3.1.14

content rights object

rights object containing a content key and pertaining to content protection

3.1.15

customer operation centre

entity responsible for billing the customer

NOTE It is assumed that the customer will have a contractual relationship with this organization.

3.1.16

device

terminal that is capable of receiving broadcast transmission over broadcast network

NOTE The terminal may be capable of interacting with a service provision subsystem and a commerce subsystem through a cellular network. The terminal may include optional embedded secure hardware, such as a UICC.

3.1.17

digital rights management

set of methods which ensures that content, during its entire lifetime, can only be used in specified ways and only when the relevant conditions (for example, access conditions) have been met

NOTE These "specified ways" and "relevant conditions" are expressed in rights objects.

3.1.18

DRM time

secure, non user-changeable time source

NOTE The DRM time is measured in the UTC time scale.

3.1.19

DVB network

network for transmitting a collection of MPEG-2 transport streams, each carrying a multiplex, and transmitted on a single delivery system

NOTE DVB network is identified by network_id.

3.1.20

electronic service guide

service guide in IPDC over DVB-H systems

3.1.21

interactive device

device that is capable of directly connecting to a rights issuer using an appropriate protocol over an interactivity channel over an appropriate transport/network layer interface, for example, HTTP over TCP/IP

3.1.22

interactive domain

OMA DRM 2.0 domain, as specified in OMA-ERP-DRM-V2_0-20060303-A

NOTE This is a group of devices for which rights objects can be issued via an interactivity channel granting rights to the whole group.

3.1.23**interactivity channel rights object**

content, programme or service rights object delivered over an interactivity channel

3.1.24**interactivity channel**

bi-directional channel established between the broadcast service network and the device for reliable exchange of messages

3.1.25**interactivity network**

network supporting bi-directional communication and the reliable delivery of messages between the device and the rights issuer

3.1.26**interactivity network cell**

cell forming part of an interactivity network

3.1.27**IP flow**

stream of IP datagrams each sharing the same IP source and destination address

3.1.28**IPDCKMSId**

identifier assigned for a particular IPDC key management system by DVB (also known as CA_system_id in ETSI ETR 162)

3.1.29**ISMACryp**

end-to-end content encryption system for media carried over RTP streams and ISO-based media files

3.1.30**key management system**

end-to-end system to authorize users and provide them the necessary means to access protected content

3.1.31**key stream message**

message broadcast alongside a protected service, carrying key material to decrypt and optionally authenticate the service

3.1.32**media access unit**

smallest data entity to which timing information can be attributed

NOTE In the case of audio, an access unit is an audio frame, and in the case of video, a picture.

3.1.33**media flow**

elementary stream or IP flow carrying audio or video data

3.1.34**metering rights object**

content, programme or service rights object used in conjunction with consumption-based charging

3.1.35

mixed-mode device

combination of a broadcast device and an interactive device

3.1.36

mobile TV application

main device application responsible for accessing the mobile TV services

NOTE This is sometimes referred to as the player application.

3.1.37

nonce

randomly chosen value, different from previous choices, inserted in a message to protect against replay attacks

3.1.38

off line

without using a direct link (such as the interactivity channel) between network entities and the device (also called "out of band")

3.1.39

OMA BCAST

working group in OMA developing a fully standardized system allowing operators to control access and usage of broadcast content on mobile devices

3.1.40

out of band

without using a direct link (such as the interactivity channel) between network entities and the device (also called "off line")

NOTE The name OOB is used in different ways in different contexts. OOB is used to signal out of band notification of data to the RI, as, for example, in registration over means other than the interactivity channel. In DVB-T/C/S systems, the term OOB or "out of band" is well known to signal a part of the spectrum other than the in band (a.k.a. IB). In the latter context, the OOB may carry data in such environments to save bandwidth for repeating messages in the IB. In the T/C/S context, DVS-167/178 or DOCSIS are well-known "OOB" systems. To make matters more complex, DOCSIS may be used as OOB when multiplexing in tables in the downstream and as interactivity channel when carrying IP data packets in Ethernet frames.

3.1.41

parameter set

either a sequence parameter set or a picture parameter set

NOTE This term is used to refer to both types of parameter sets.

3.1.42

parameter set elementary stream

elementary stream containing access units made up of NAL units for coded picture data

3.1.43

programme rights object

rights object containing a programme key or keys and pertaining to service protection

3.1.44

programme

logical portion of a service with a distinct start and end

3.1.45

rights issuer context

context consisting of information that was negotiated with a given rights issuer, during the 4-pass registration protocol such as the rights issuer ID, rights issuer certificate chain, version, algorithms used and other information

NOTE A right issuer context is necessary for a device to participate successfully in all the protocols of the ROAP suite, except the registration protocol.

3.1.46

rights issuer service

IP datacast channel used to carry broadcast rights objects, registration data and other messages from a rights issuer over a broadcast channel

3.1.47

rights issuer

entity that registers devices and provides rights objects allowing devices to receive protected services

3.1.48

rights object

collection of permissions, keys and other attributes that are linked to items of content or services

3.1.49

roaming

end-user accessing IPDC services through another ('foreign') service provider than the 'home' service provider

NOTE Roaming is usually based on roaming agreements between service providers.

3.1.50

service

one or more IP flows intended to be presented together

NOTE Examples include, but are not limited to, audio and video services.

3.1.51

service guide

data source describing the services and content available via a network and how they can be received

3.1.52

service operation centre

service provider

NOTE See also other definitions with 'service'.

3.1.53

service protection

protection of a service such that only authorized devices are able to receive and decode it

3.1.54

service provider

provider of a broadcast service – the entity that broadcasts the service, and provides key and schedule information to rights issuers

3.1.55

service rights object

rights object containing one or multiple service keys and pertaining to service protection

3.1.56

service roaming

roaming during which the user has access to the same services as through the home service provider

3.1.57

simulCrypt

system that provides the ability for multiple KMSs to control access at the same time to a single content stream

3.1.58

super distributable content

protected (encrypted) content that can be freely distributed and for which the recipients can obtain ROs from an RI for the consumption of that content, because that protected (encrypted) content has a link to the RI in it as well as enough information such that the RI can determine the decryption key

3.1.59

terminal

consumer device that can receive, descramble, and decode services

3.1.60

token rights object

special interactivity channel rights object containing tokens for pre-/post-paid consumption-based charging of interactive devices, or a special broadcast rights object containing tokens for pre-/post-paid consumption-based charging of broadcast devices

3.1.61

unconnected device

device, as defined in OMA-AD-DRM-V2_0-20060303-A, which cannot connect direct to a rights issuer via an interactivity channel for the acquisition of rights objects, but can do so via an intermediary device

3.1.62

user

person using the device to receive protected services

3.1.63

user roaming

roaming during which the user has access to the services of the foreign service provider

3.1.64

video elementary stream

elementary stream containing samples made up of only sequence and picture parameter set NAL units synchronized with the video elementary stream

3.2 Symbols

For the purposes of this document, the following symbols apply.

$E\{K\}(M)$	Encryption of message 'M' using key 'K'
$D\{K\}(M)$	Decryption of message 'M' using key 'K'
P	Public key
Q	Private key
RIQ	Rights issuer private key
RIP	Rights issuer public key
DQ	Device private key
DP	Device public key
$A\{K\}(M)$	Authentication of message 'M' with key K
$V\{K\}(M)$	Verification of message 'M' with key K
$A==B$	Yields true if and only if A equals B
$A\&\&B$	Yields true if and only if both A and B are true

$A \& B$	Bit-wise AND of A and B
$A \oplus B$	Bit-wise exclusive OR of A and B
$A B$	Bit-wise OR of A and B
$A B$	Concatenation of A and B
$A + B$	Arithmetic addition in case A and B are numerical arguments; concatenation of A and B if A and B are strings
$A << B$	Bit-wise shift left operation of A by B bits, filling with 0s
$A >> B$	Bit-wise shift right operation of A by B bits, filling with 0s
LSBm(X)	The bit string consisting of the <i>m</i> least significant bits of the bit string X
MSBm(X)	The bit string consisting of the <i>m</i> most significant bits of the bit string X

3.3 Abbreviations

For the purposes of this document, the following abbreviations apply

ACG	Access Criteria Generator
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AID	Application Identifier
APDU	Application Protocol Data Units
API	Application Program Interface
ARC	Action Request Code
ASCII	American Standard Code for Information Interchange
ATM	Asynchronous Transfer Mode
AU	Access Unit
AVC	Advanced Video Codec
AVP	Attribute-Value Pairs
BAK	BCRO Authentication Key
BCD	Binary Coded Decimal
BCG	Broadband Content Guide
BCI	Binary Content ID
BCRO	Broadcast Rights Object
BDK	Broadcast Domain Key
BOC	Broadcast Operation Centre
bslbf	bit string left bit first
CA	Conditional Access
CAS	Conditional Access System
CAT	Conditional Access Table
CBC	Cipher Block Chaining
CCI	Copy Control Information
CDC	Connected Device Configuration
CDP	Content Delivery Protocol
CEK	Content Encryption Key
CGF	Customer Group Filter
CLDC	Connected Limited Device Configuration
CID	Content ID
CIEK	Content Item Encryption Key
COC	Customer Operation Centre
CoD	Content on Demand
CPCM	Content Protection and Copy Management
CRC	Cyclic Redundancy Check

CRL	Certificate Revocation List
CSA	Common Scrambling Algorithm
CTR	Counter
DCF	DRM Content Format
DEK	Daily Encryption Key
DIST Mgmt	Service Distribution Management
DOCSIS	Data Over Cable Service Interface Specification
DRD	Device Registration Data
DRM	Digital Rights Management
DVB	Digital Video Broadcasting
DVB-C	DVB-Cable
DVB-H	DVB-Handheld
DVB-IP	DVB-Internet Protocol Infrastructure
DVB-S	DVB-Satellite
DVB-T	DVB-Terrestrial
ECB	Electronic Code Book
ECM	Entitlement Control Message
ECMG	ECM Generator
EIS	Event Information System
EIT	Event Information Table
EMM	Entitlement Management Message
EMMG	EMM Generator
EPG	Electronic Programme Guide
ESG	Electronic Service guide
ESP	Encapsulating Security Payload
GCF	Generic Connection Framework
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HMAC	Hashed Message Authentication Code
HO	Home Operator
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure – Hyper Text Transfer Protocol
IC	Interactivity Channel
ICRO	Interactivity Channel Rights Object
ID	Identifier
IEK	Inferred Encryption Key
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPDC	IP DataCast
IPPV	Impulse Pay Per View
IPsec	IP Security
IPTV	Internet Protocol Television
IRD	Inform Registered Device (protocol)
IrDA	Infrared Data Association
ISMA	Internet Streaming Media Alliance
ISO	International Standards Organization
IV	Initial Vector
KML	Key Management Layer
KMM	Key Management Message

KMS	Key Management System
KSL	Key Stream Layer
KSM	Key Stream Message
LBDF	Long-form Broadcast Domain Filter (a.k.a. longform_domain_id)
lsb	least significant bit
MAC	Message Authentication Code
MF	Master File
MII	Major Industry Identifier
MIME	Multipurpose Internet Mail Extensions
MJD	Modified Julian Date
mjdutc	Modified Julian Date UTC
MK	Master Keys
MKI	Master Key Indicator
MPEG	Moving Pictures Experts Group
MPTS	Multi Program Transport Stream
msb	most significant bit
MSISDN	Mobile Station Integrated Services Digital Network
MTU	Maximum Transmission Unit
NAL	Network Abstraction Layer
NDD	Notification of Detailed Data
NIST	National Institute of Standards and Technology
NIT	Network Information Table
NSD	Notification of Short Data
OBEX	Object Exchange Protocol
OCSP	Online Certificate Status Protocol
OMA	Open Mobile Alliance
OOB	Out Of Band
OTA	Over The Air (i.e. transfer over a wireless connection)
PAK	Programme Authentication Key
PAS	Programme Authentication Seed
PAT	Programme Association Table
PCT	Purchase Channel Table
PDCE	Packetised DRM Content Format
PDR	Push Device Registration
PEAK	Programme Encryption/Authentication Key/Seed

NOTE Concatenation of PEK and PAS.

PEK	Programme Encryption Key
PES	Packetised Elementary Stream
PID	Packet Identifier
PIT	Purchase Item Table
PKC	Public Key Certificate
PKCS	Public-Key Cryptography Standards
PKC-ID	PKC Identifier: the hash of the Public Key Certificate
PKI	Public Key Infrastructure
PMT	Programme Map Table
PPV	Pay Per View
PS	Program Stream
PSI	Programme Specific Information
PSS	Probabilistic Signature Scheme

RI	Rights Issuer
RIAK	Right Issuer Authentication Key
RID	Registered application provider Identifier
RIS	Rights Issuer Services
RML	Rights Management Layer
RO	Rights Object
ROAP	Rights Object Acquisition Protocol
ROC	Roll-Over Counter
ROT	Root Of Trust
rpchof	remainder polynomial coefficients, highest order first
RSA	Rivest-Shamir-Adleman public key algorithm
RSASSA-PSS	RSA Signature Scheme with Appendix - Probabilistic Signature Scheme
RTP	Real-time Transport Protocol
SA	Security Association
SAC	Secure Authenticated Channel
SAK	Service Authentication Key
SAS	Service Authentication Seed
SBDF	Short-form Broadcast Domain Filter (a.k.a. shortform_domain_id)
SBT	Service Bundle Table
SCS	SimulCrypt Synchronizer
SDP	Session Description Protocol
SDT	Service Description Table
SEAK	Service Encryption / Authentication Key / Seed
	NOTE: Concatenation of SEK and SAS.
SEK	Service Encryption Key
SG	Service guide
SGK	Subscriber Group Key
SHA-1	Secure Hash Algorithm
SI	Service Information
SIM	Subscriber Identity Module
SK	Session Key
SMS	Short Message Service
SOC	Service Operation Centre
SPI	Security Parameters Index
SPP	Service Purchase and Protection
SRTP	Secure Real-Time Transport Protocol
SUB Mgmt	Service Subscription Management
TAA	Trust Authority Algorithm
TAK	Traffic Authentication Key
TAS	Traffic Authentication Seed
TDK	Token Delivery Key
TDRMAK	Token Delivery Response Message Authentication Key
TEK	Traffic Encryption Key
TS	Transport Stream
UDF	Unique Device Filter
UDK	Unique Device Key
UDN	Unique Device Number
UDP	User Datagram Protocol
UGK	Unique Group Key

UICC	Universal Integrated Circuit Card
uimsbf	unsigned integer, most significant bit first
UMTS	Universal Mobile Telecommunications System
UPnP	Universal Plug and Play
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
UTC	Universal Time Coordinated
UTF	Unicode Transformation Format
UTF-8	8-bit Unicode Transformation Format
VO	Visited Operator
VM	Virtual Machine
WAP	Wireless Application Protocol
WIM	WAP Identify Module
XML	eXtensible Markup Language
ZMB	Zero Message Broadcast

3.4 Identifiers assigned by external entities

18CRYPT_CAS_ID: This is the CA_system_id assigned to 18Crypt by the DVB project. The value can be found at

ETSI ETR 162: http://www.dvb.org/products_registration/dvb_identifiers/

18CRYPT_PRIVATE_DATA_ID: This is the private data identifier ID assigned to 18Crypt by the DVB project. The value can be found at

ETSI ETR 162: http://www.dvb.org/products_registration/dvb_identifiers/

4 General

This clause provides a general introduction to this standard. This clause covers

- the service purchase and protection system;
- the four-layer model for service protection;
- the end-to-end system and use of broadcast and interactivity channels;
- the types of systems and devices supported by this standard;
- difference between service and content protection.

The specification subsequent to the present clause is structured as follows.

- Clause 5 provides general specifications and concepts for the service purchase and protection system.
- The four-layer model is specified in 5.4. The four layers are specified in Clauses 6, 7, 8 and 9 respectively.
- Clause 10 specifies signalling and service and content discovery (service guide – SG).
- Clause 11 specifies the RI services, i.e. the system with which messages meant for individual devices or groups of devices are broadcast.
- Service purchase is specified in Clause 12.
- The subsequent clauses provide normative prescriptions specific for the individual supported systems, which are:

- IPDC over DVB-H systems, Clause 13;
- DVB T/C/S systems, Clause 14;
- MPEG2 TS-based IP systems, Clause 15;
- Non-MPEG2 TS-based IP systems, Clause 16.

Annex A normatively specifies several required tools and technologies in detail.

Annex B may provide the reader with more insight into the system.

4.1 General description of the system and elements

This standard specifies a service purchase and protection system for services transmitted over a broadcast infrastructure. It enables access to services to be restricted to authorized users.

The solution can operate on either

- the Internet protocol (IP) level, based on the IPsec security standard, in which case it is transparent to IP-based applications (such as video players); or
- the transport layer, depending on the application using SRTP, ISMACryp, or MPEG2 TS CRYPT. This allows direct storage of the content in encrypted form.

Additional application-specific content protection mechanisms could be freely combined with this solution, if desired, on top of the transport layer.

OMA DRM 2.0 is used as the default framework for rights management. In its most common form, OMA DRM 2.0 manages the rights to use files stored in a device; this standard extends that to the case of receiving streaming content over a broadcast channel. It also provides a means of performing rights management over a broadcast channel.

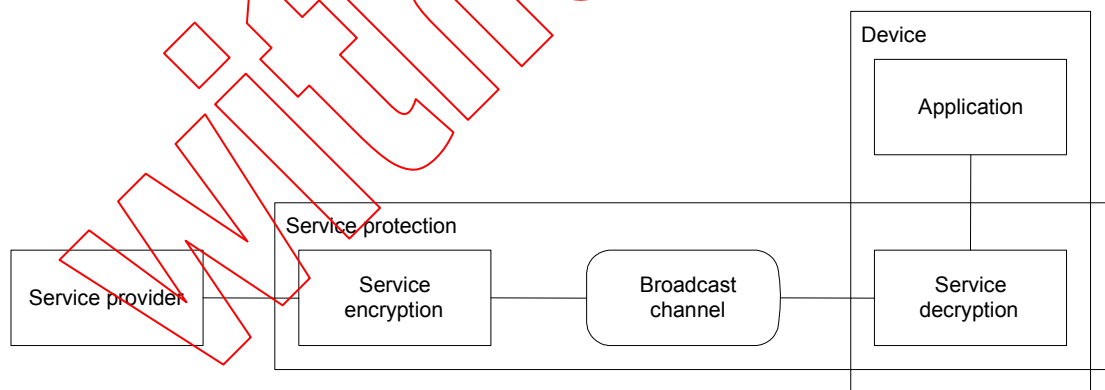


Figure 1 – System overview

Figure 1 shows the position of the service protection system within the overall architecture. IPsec allows the solution to be completely independent of the content format, while SRTP, ISMACryp and MPEG2 TS CRYPT provide alternatives for protecting content at the transport layer. Depending on the mode of operation, different normative prescriptions apply for the selection between the three ciphers. This is specified in the clauses about the supported systems.

4.1.1 Selected technologies

The following are the main standards on which the solution is based.

- Advanced Encryption Standard (AES, see FIPS PUB 197:2001) in the cipher block chaining mode, for actual content encryption. Furthermore, OMA DRM uses AES-WRAP in its rights objects and optionally AES CBC-MAC.
- Secure Internet Protocol (IPsec, see IETF RFC 4301) using the encapsulating security payload (ESP) protocol, for implementing service encryption and decryption as a function of the IP stack. Only the transport mode is used.
- Secure Real Time Protocol (SRTP, see IETF RFC 3711) as one option for implementing service protection at the transport layer. SRTP uses AES-CTR (counter mode).
- ISMA Encryption and Authentication, see ISMACryp 2.0, as a second option for implementing service protection at the transport layer. ISMACryp also uses AES-CTR (counter mode).
- The DVB-CSA as well as DES, 3DES, AES and M2 ciphers as the options for encrypting content in an MPEG2 TS.
- A traffic key delivery protocol and management as specified in this standard.
- Open Mobile Alliance (OMA) Digital Rights Management version 2.0 (OMA DRM 2.0, see OMA-ERP-DRM-V2_0-20060303-A) for managing rights to services, the associated service keys and the cryptographic protection of those keys themselves. This standard introduces some adaptations to OMA DRM 2.0 for IPDC service protection.
- Rights object delivery and device registration over a broadcast channel, without making any use of an interactivity channel, are also specified in this standard.
- Adapted Zero Message Broadcast according to Fiat Naor:1998 in 1-resilient mode.
- SimulCrypt (see ETSI TS 103 197) head-end interfaces.

The reasons for choosing these particular technologies as the basis of the solution include the following.

- AES is an efficient symmetric encryption method and an open standard that has hardware implementations. AES has many existing applications.
 - IPsec/ESP is the standard way of keeping service decryption in receiving devices within the IP stack, invisible to the receiving applications, which thus remain independent of service protection and the carriers of the IP flows.
- NOTE An IPDC specific broadcast channel is only one means to transmit such IP flows. IPsec/ESP has many existing applications.
- SRTP is a standard way of performing service decryption at receiving devices within the transport layer. It can be used to carry all common forms of streaming content, which can be stored by a device for later decryption, if required.
 - ISMACryp is also a standard way of performing service decryption within the transport layer. It provides end-to-end protection for transport and storage of streaming content.
 - DVB-CSA is a widely deployed, standard way of encrypting content in an MPEG2 TS. The descramblers of most video processors implement the alternative DES, 3DES, AES and M2 ciphers.
 - The traffic key (i.e., the actual content encryption key) management framework and protocol are specified in this standard. The efficiency and robustness of the solution is achieved by a particular delivery protocol and management scheme for the frequently changing traffic keys.
 - OMA DRM2.0 is a state-of-the-art open standard for digital rights management. The use of OMA DRM2.0 allows deployments to leverage existing implementations in the area of DRM-enabled services.
 - OMA DRM 2.0, however, uses interaction over a two-way communication channel for device registration and guaranteed rights delivery. To adapt to broadcast devices, and to optimize the use of the broadcast channel, some new standardization is introduced.
 - The main and foremost consideration for the system is network bandwidth efficiency, while maintaining realistic CPU requirements for the local device. By using zero message

broadcast encryption, the network does not need to transmit keys to devices after registration. By choosing Fiat Naor, there is a good balance between network bandwidth consumption and local device processing requirements.

The chosen group size is relatively small (with 256 or 512 devices), and, depending on the group size(m), the following is needed:

- device transmission and storage for $2\log(m)$ subscriber group keys (a.k.a. 'SGKs');
- device computing power to derive (m-1) leaf keys;
- device computing power to process, worst case, (m-1) leaf keys to create the "IEK" key that covers the SEK.

Given the small size of the subscriber group, local device processing requirements are not considered a problem.

Fiat Naor is used in 1-resilient mode, thereby making a collusion attack in theory possible. Making the scheme k-resilient, as discussed in Fiat Naor:1998 will increase the number of keys dramatically. The potential threat of 1-resilience is countered by measures described in 5.5.3.

- By using SimulCrypt interfaces for the T/C/S head-end, the 18Crypt solution can be easily integrated into existing DVB head-end configurations by using widely available SimulCrypt components.

4.1.2 Overview of four-layer model for service protection

This subclause introduces the four-layer model for service protection. The four-layer model is specified in 5.4. The four layers are specified in Clauses 6, 7, 8 and 9, respectively.

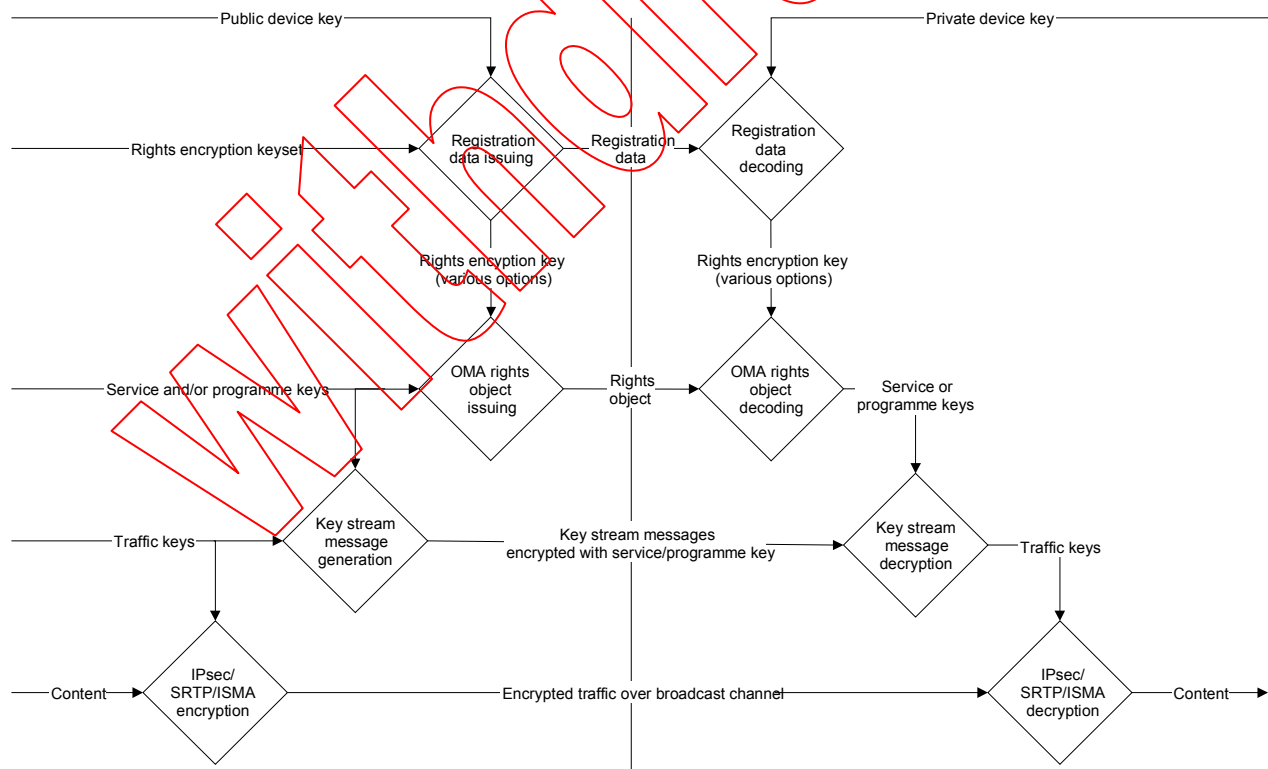


Figure 2 – Service protection via four-layer model

As illustrated in Figure 2, the solution is based on a four-layer cryptographic architecture, with an optional optimization to provide both secure subscription and pay-per-view purchase options for a single service. Actual service encryption is carried out according to AES using 128-bit symmetric traffic keys.

Traffic keys are applied

- as part of standard IPsec security associations (SAs); or
- as an SRTP master key, from which the session key is derived according to the SRTP specification; or
- as an ISMACrypKey, from which the session key is derived according to the ISMACryp specification; or
- as a content key for MPEG2 TS CRYPT.

These are used by the IPsec, SRTP, ISMACryp or MPEG2 TS CRYPT layers to perform decryption automatically before passing the packets to the receiving application. The traffic keys are not protected by IPsec, but instead encrypted with a service or programme key on the key stream layer, above the IP socket interface. These broadcast messages carrying traffic keys are called key stream messages.

Key stream messages can contain two levels of encryption. Separate programme and service keys have different lifetimes and can be used to provide, for a single service, different granularities of purchase periods to different users. This allows for the efficient implementation of both subscription and pay-per-view business models for the same service. Pay-per-view customers are provided with a programme key that is only valid for a single programme while subscribers are given a service key, valid for reception of the service for some longer period. Within the key stream message, the traffic key is encrypted with a programme key, and the programme key is also carried, encrypted with the service key. Thus, pay-per-view customers can directly decrypt the traffic key, while subscribers can decrypt the programme key using the service key, which can then be used to decrypt the traffic key.

Key stream messages contain extensions to content IDs, which are carried in the service guide, for the programme and/or service. Devices use this ID to identify which rights object contains the keys to use for key stream message decryption.

Where the two-level service and programme functionality is not required, the traffic key can be directly encrypted with either the service or programme key with the service-key-encrypted programme key omitted.

The service or programme key(s) are transmitted to each receiving device within OMA DRM 2.0 rights objects (ROs). Such transmission of ROs can be done in two different ways, depending on whether the receiving device can make use of a separate interactivity channel:

- via a broadcast channel; or
- by using the separate interactivity channel.

In both cases, the ROs can be utilized by the customer device only, since the service or programme key sections are protected according to the OMA DRM 2.0 standard, or, in the broadcast case, by the variant of OMA DRM 2.0 specified in this standard.

When delivering rights objects over a broadcast channel, bandwidth is a major constraint. This standard addresses this problem in two complementary ways. Firstly, a new binary form of the OMA DRM 2.0 rights object, called a broadcast rights object (BCRO), is defined. Secondly, a method is specified for securely delivering BCROs to groups of devices using a single broadcast message. Valuable portions of rights objects are protected by group or unit keys, and when necessary, zero message broadcast encryption can be used to allow messages to be decrypted only by arbitrary sets of devices within a larger group.

An additional mechanism is available, as in OMA DRM 2.0, for rights objects to be issued to a group of devices known as a domain. It is expected that a domain will contain a number of devices belonging to the same user, and will be used by rights issuers to sell subscriptions allowing all devices within the domain to receive protected services.

Registration can be performed either via an interactivity or via a broadcast channel. In the case that an interactivity channel is used, the registration protocol is according to OMA DRM 2.0 and unit keys are delivered, protected with the public key of the device. This standard defines an efficient and user-friendly process for the registration of devices that do not support an interactivity channel, and a new protocol, called the 1-pass ROAP, is defined for the delivery of unit, group and broadcast keys via a broadcast channel.

The service key protection thus is based, according to OMA DRM 2.0, on a public key cryptosystem where the public key of the customer device is registered at each rights issuer and the corresponding private key is kept within the customer device.

4.2 End-to-end system

This subclause briefly specifies the major roles within the system. For more details, see 5.1.

Figure 3 shows a simplified view of the major actors in the system and their relationship to each other.

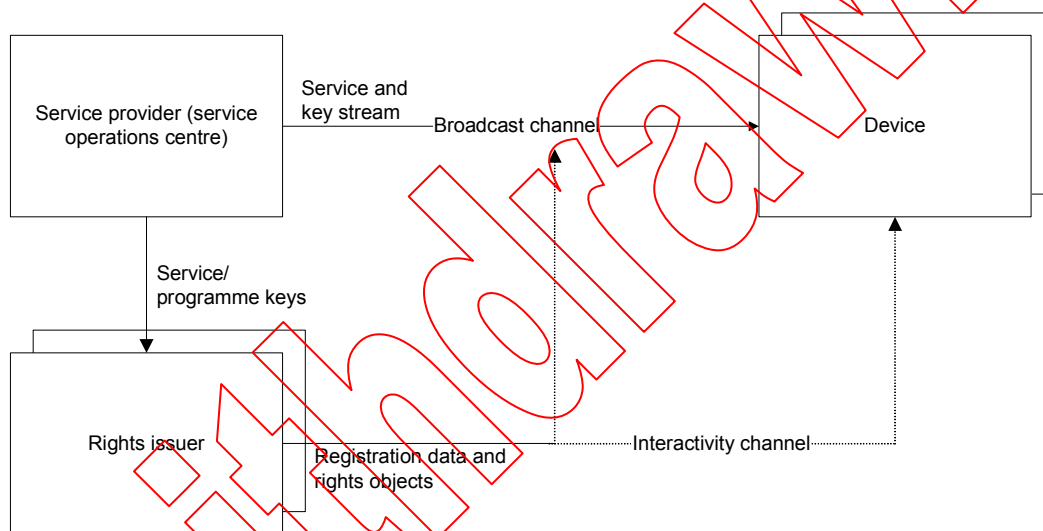


Figure 3 – Highly simplified view of the end-to-end system

The main actors are as follows.

- The service provider, also known as the service operations centre, broadcasts and encrypts the service and the key stream. It provides service and programme keys to the rights issuers.
- The rights issuer registers devices and provides rights objects to registered devices allowing them to decrypt the services that they are entitled to receive.
- The device receives the service, decrypts it (if it has the necessary rights objects) and presents it to the user.

4.3 Supported systems and device types

This standard supports stream based service access for the following systems.

- IP datacast over DVB-H, referred to in this standard as 'IPDC over DVB-H system'.
- Digital broadcast system according to DVB-T, DVB-C or DVB-S standard, referred to in this standard as 'DVB T/C/S system'.
- Two versions of IPTV:
 - MPEG2 TS-based IP system;

- non-MPEG2 TS-based IP system.

Based on the communication channels used, this standard supports the following device types, as listed in Table 1.

Table 1 – Supported systems and device types

System	IPDC over DVB-H			DVB T/C/S		IP	
						MPEG2 TS-based	Non-MPEG2 TS-based
See	Clause 13 Subclause B.1.1			Clause 14 Subclause B.1.2		Clause 15 Subclause B.1.3	Clause 16 Subclause B.1.3
	Broadcast device	Mixed-mode device	Interactive mode device	Broadcast device	Mixed-mode device	IPTV device	IPTV device
Comm. channel(s)	IPDC	IPDC + IC	IC	DVB-T/C/S	DVB-T/C/S + (optional) IC	IC	IC
AV content (Traffic layer, Clause 6)	Via SRTP or IPsec over IP	Via SRTP or IPsec over IP	Via SRTP or IPsec over IP	Via PES over MPEG2 (MP)TS	Via PES over MPEG2 (MP)TS	MPEG2 AV data via PES over IP	Via SRTP, IPsec or ISMACryp over IP
TEK (Key stream layer, Clause 7)	KSM via IP (packets)	KSM via IP (packets)	KSM via IP (packets)	KSM via SI table (section) in TS	KSM via SI table (section) in TS	KSM via MPEG2 table (section) in TS	KSM via IP (packets)
RO (Rights management layer, Clause 8)	BCRO via IP packets using RI services (Clause 10)	BCRO via IP packets over IPDC or ICRO via XML/ROAP over IP or OBEX	ICRO via XML/ROAP over IP or OBEX	BCRO via SI table (section) in TS, using RI services (Clause 10)	BCRO via SI table over TS or ICRO via XML/ROAP over IP or OBEX	ICRO via XML/ROAP over IP	ICRO via XML/ROAP over IP
Registration data (Registration layer, Clause 9)	Via IP packets, using RI services (Clause 10)	Via IP packets over IPDC or via XML/ROAP over IP or OBEX	Via XML/ROAP over IP or OBEX	Via MPEG2 tables (sections) in TS, using RI services (Clause 10)	Via MPEG2 tables (sections) in TS or via XML/ROAP over IP or OBEX	Via XML/ROAP over IP	Via XML/ROAP over IP
Service guide (Clause 10)	IPDC over flute	IPDC over flute	IPDC over flute	Purchase and EPG data via extra SI tables plus DVB-SI or A65 in TS	Purchase and EPG data via extra SI tables plus DVB-SI or A65 in TS; optionally as additional programme information data over IC	DVB-IPI BCG	DVB-IPI BCG

NOTE DVB-T/C/S devices may use linkage descriptors for more options to signal where the messages will be carried, as explained in B.6.2. This has been omitted in this table for the sake of clearness.

4.4 Service protection versus content protection

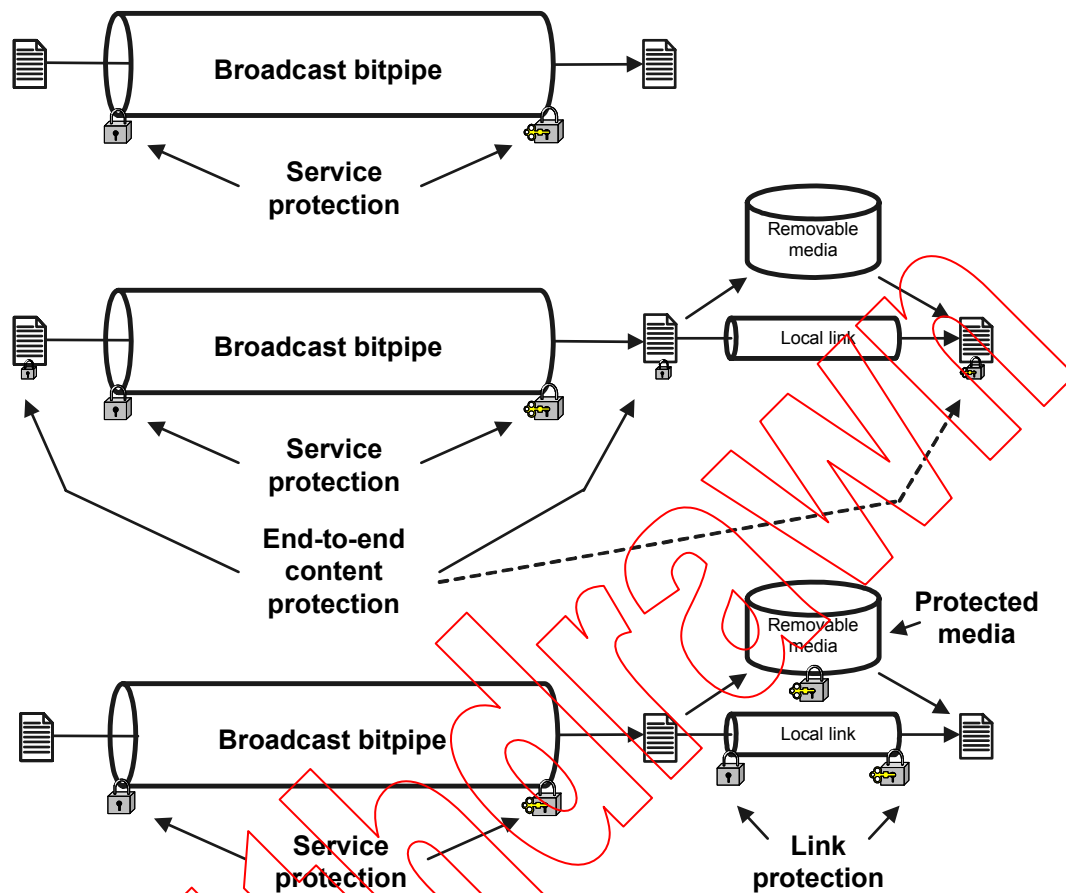


Figure 4 – Service protection versus content protection

Figure 4 illustrates the conceptual difference between service protection and content protection.

Service protection ensures that only those authorized to access the broadcast service can do so. Service protection is removed at reception time.

Content protection refers to protecting the content either throughout the content lifecycle (end-to-end content protection) or subsequent to delivery through the service protection system (post-delivery content protection).

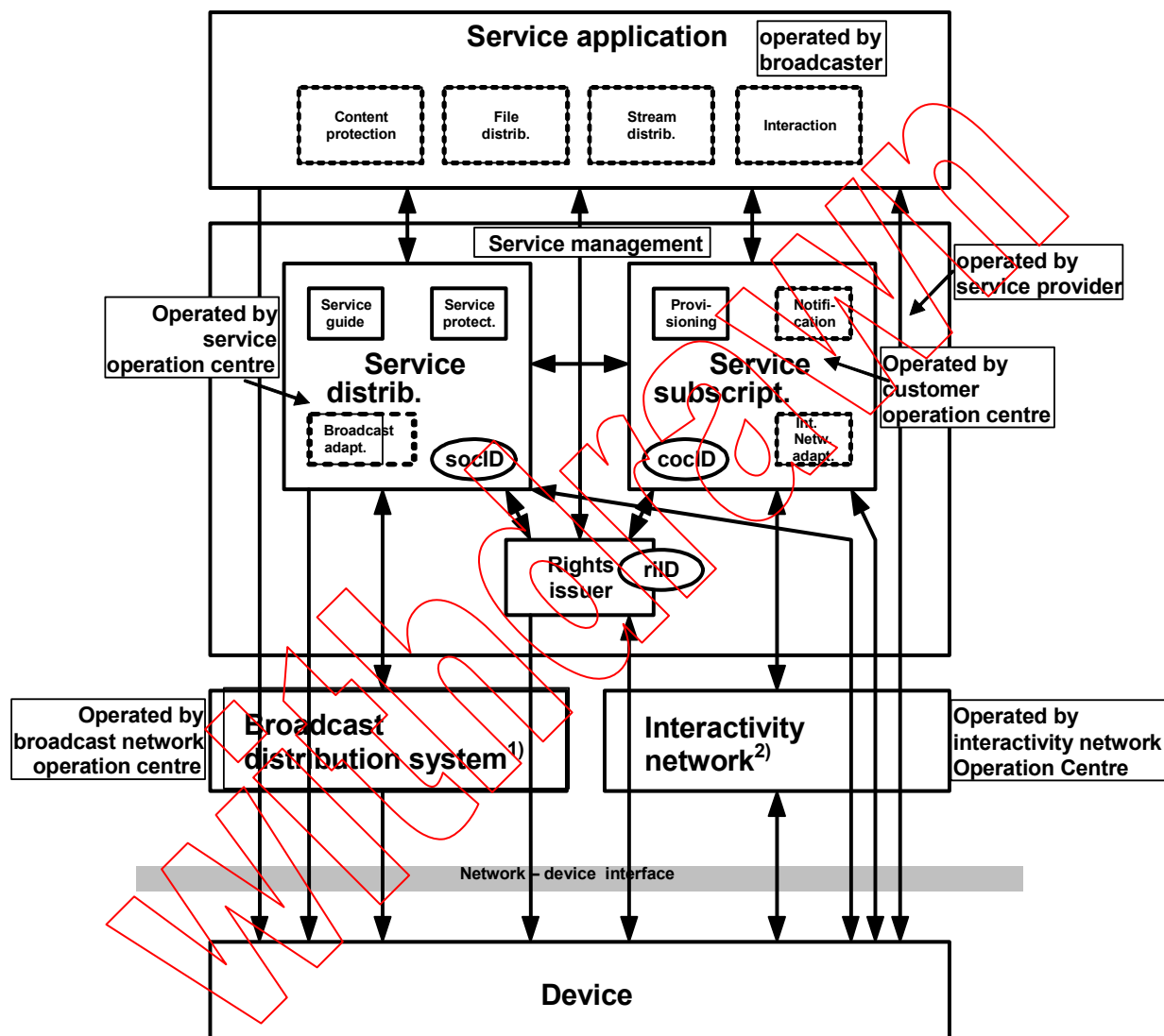
The services purchase and protection system defined in the present standard provides service protection, and it can optionally also be used to facilitate end-to-end content protection. The access permission in rights objects controls access to the broadcast service and allows immediate rendering of the content. In order to be able to play recorded content, play permission is required. If only service protection is needed, export permission can be used to allow exporting in the clear.

In some cases, for instance to facilitate sharing of the protected content with different devices, it could be desirable to export the content to a separate post-delivery content protection system. The usage state information needed by such a content protection system can be carried as a constraint for export permission.

5 General specifications

5.1 End-to-end architecture

This subclause specifies the end-to-end architecture of the system in a network centric way and illustrates how the public key infrastructure relates to the end-to-end architecture. The figures in this subclause can be used as a reference and overview when reading this standard.



NOTE 1 Broadcast distribution systems may be:

- IP datacast over DVB-H;
- digital broadcast system using the DVB-T, DVB-C or DVB-S standard;
- the Internet.

NOTE 2 Interactivity networks may be:

- cellular radio networks like GSM/GPRS;
- ADSL, ATM or DOCSIS networks;
- the Internet.

Figure 5 – Service protection and purchase entities and names (broadcast architecture)

Figure 5 names several entities used in this standard. The arrows in this figure represent information flow between the elements. All these entities should be considered as logical entities, i.e. actual deployment may be different and entities indicated separately in Figure 3

may well be merged into larger systems. One should also note that there may be additional connections and entities, such as the off-line communication of broadcast mode devices and certification authority needed for public key infrastructure.

The service application represents any content that can be sent over a broadcast channel. Besides digital television it can be, for example, discrete files, streams or interactive services. The service distribution management's role is to create and manage protected broadcasts as specified in this standard. Service subscription management takes care of the purchase of services. The rights issuer takes care of device registration and rights issuing.

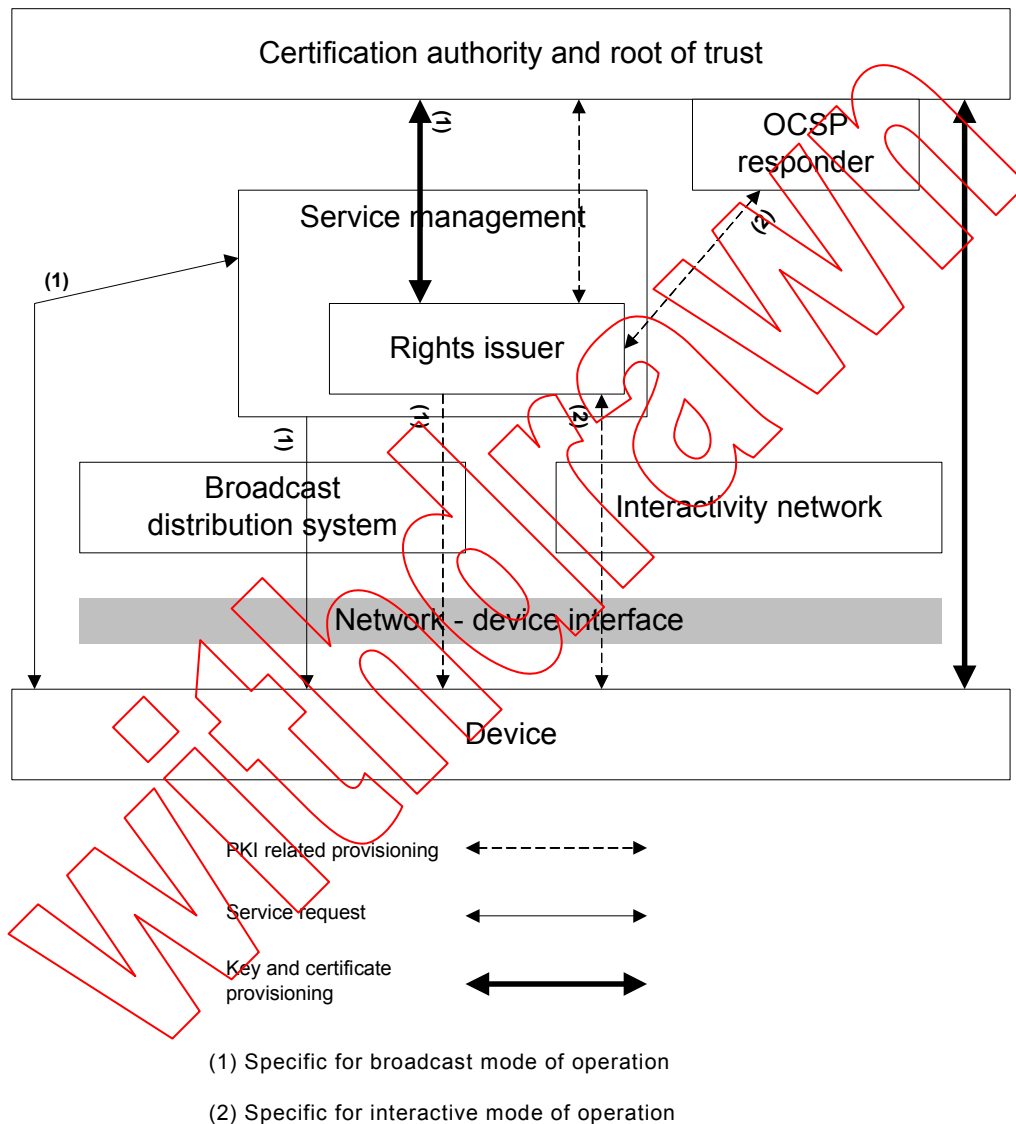


Figure 6 – Public key infrastructure

Figure 6 maps entities from the public key infrastructure to the broadcast architecture. A root certification authority provides keys and certificates to devices and rights issuers. If the device and rights issuer do not have the same root certification authority, the rights issuer cannot register the device or issue rights to the device.

Lines marked with (1) relate to the broadcast mode of operation and lines marked with (2) relate to the interactive mode of operation (compare Figure 6 with Figure 22 and Figure 37).

5.2 Special cases

5.2.1 Free-to-air services

Free-to-air services, by definition, are broadcast without any service protection. Any device can receive these services. In this subclause, 'air' may also mean 'cable', etc.

- Free-to-air services shall not be broadcast using IPsec, SRTP, ISMACryp or MPEG2 TS CRYPT. In this case, a key stream will not normally be broadcast, but if one is broadcast, it shall be ignored by the device.

Otherwise, free-to-air services are beyond the scope of this standard.

5.2.2 Free-to-view services

Free-to-view services are broadcast with service protection, but no charge is made to receive the services. However, reception can be restricted to certain users.

It is expected that free-to-view services will be implemented by either

- requiring users to "subscribe" to the service in the normal way, although no charge is made for the subscription (rights objects are delivered to "subscribers"); or
- distributing rights objects to all devices in a population or to particular pre-existing subscriber groups or registered devices without requiring a specific "subscription".

However, free-to-view services may be implemented in any way that is compliant with this standard.

5.3 Service guide and purchase

Broadcast systems may have some form of service guide available. This service guide is a source of service, programme and content information. Service and content discovery may then be based on information transmitted in the service guide.

In systems supporting automated purchase of services and content, it is assumed that a service guide is available, which also contains necessary information for making a purchase of a service or programme. This means that for each service and programme, the service guide contains all the necessary information for making a purchase and for the device to find services and programmes.

NOTE "Service guide" is used as a generic term in this standard. Specific systems may use specific terms (for example, ESG in IPDC over DVB-H systems; see 13.5).

Figure 7 illustrates a high-level overview of a service guide and purchase system. Line (1) in Figure 7 represents the broadcast of a service guide over a broadcast channel. Lines (4) and (5) represent purchase and lines (2) and (3) represent the delivery of necessary rights objects.

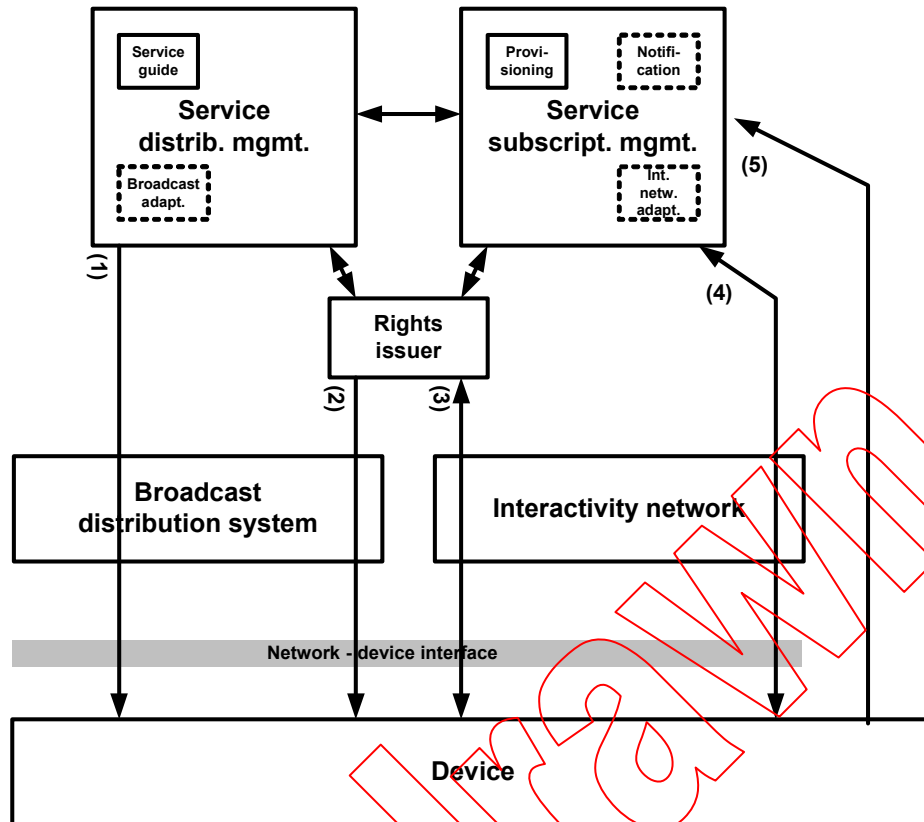


Figure 7 – Overview of service guide and purchase

Service guide data may be carried over a broadcast or interactivity channel. To be able to use the protected services and content specified in this standard, a device needs to be able to receive and parse service guide data. Unless the service or content is free to air (see 5.2.1), the user needs to make a purchase and the service guide contains all the needed information to do so. Interactive and mixed-mode devices can find the URI and other necessary parameters from the service guide. For broadcast devices, the service guide contains a ServiceID (see B.2.5.2) that identifies a purchased service or content. Line (4) in Figure 7 represents purchase by interactive and mixed-mode devices over an interactivity channel and line (5) represents off-line purchase by broadcast devices.

With interactive and mixed-mode devices, a purchase initiates the sending of an ICRO over an interactivity channel; line (3) in Figure 7. With broadcast and mixed-mode devices, BCROs are sent over a broadcast channel. Before purchases can happen, devices need to be registered with the relevant rights issuer; see Clause 9.

For more information on service guides, see Clause 10 for general specifications and 13.5, 14.5, 15.6 and 16.5 for system specific specifications.

5.4 Four-layer model – Key hierarchy

A four-layer key hierarchy is used to implement service protection. This four-layer model is analogous to the one used for protection in DVB systems. The four layers are as follows.

- a) Traffic layer (content encryption; DVB equivalent is the CSA layer).
- b) Key stream layer (DVB equivalent is the ECM layer).
- c) Rights management layer (DVB equivalent is the EMM layer).
- d) Registration layer.

The information in the traffic layer and the key stream layer is transmitted over a broadcast channel. The information in the rights management and registration layer may be distributed over a broadcast channel and/or an interactivity channel. The remainder of this subclause specifies the key hierarchy. Specific specifications of each of the layers can be found in Clauses 6, 7, 8 and 9, respectively. The way these layers are used in specific systems is specified in Clauses 13, 14, 15 and 16.

5.4.1 Keys on the traffic layer

On the lowest level, the data shall be encrypted using one of IPsec, SRTP, ISMACryp, or MPEG2 TS CRYPT, depending on the application. This layer is called the traffic layer. The key used to encrypt the traffic on this layer is called traffic encryption key, or TEK. The TEK changes frequently in the order of once per minute to once per second.

The encryption of the content can be written as

$$E\{TEK\}(C)$$

with C being the data and $E\{TEK\}()$ being the encryption function using the key TEK.

The data can be recovered by using the decryption function $D()$ with the same key TEK:

$$C = D\{TEK\}(E\{TEK\}(C))$$

As a symmetric encryption is used to encrypt the data, the data is recovered using the same key.

5.4.2 Keys on the key stream layer

The TEK itself is transmitted on the key stream layer. The TEK shall be encrypted using either a programme encryption key (PEK) or a service encryption key (SEK). The use of two different keys to protect the TEK allows for the models specified in the following three subclauses to be used.

5.4.2.1 Service-based subscription

If the service is made available to customers by subscription only, the following applies.

- If access rights change per programme, a programme key is used within the key stream message but is never delivered separately in a rights object. The scheme specified in 5.4.2.2 shall be used.
- If access rights do not change per programme, a programme key shall not be used and the scheme below shall be followed.

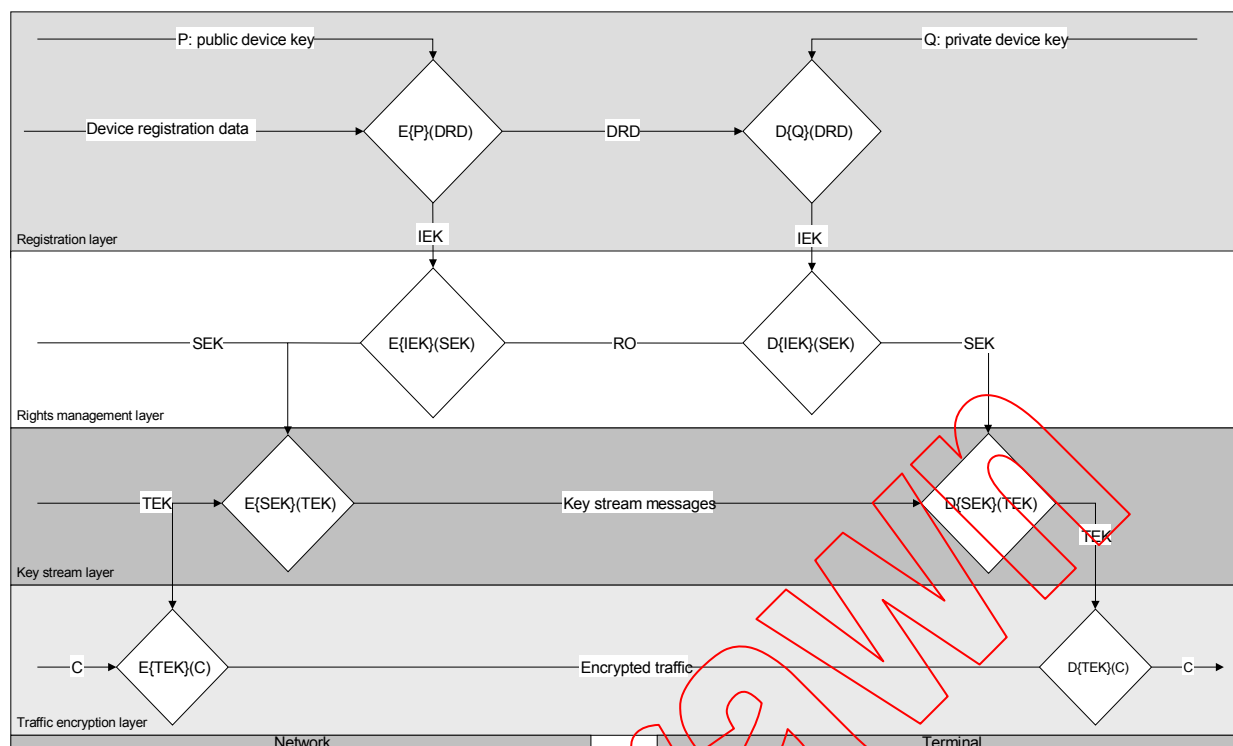
$$E\{SEK\}(TEK)$$

and

$$TEK = D\{SEK\}(E\{SEK\}(TEK))$$

The SEK is transmitted to devices as part of the rights objects on the rights management layer. These ROs shall be either normal OMA DRM 2.0 ROs in the case of an interactive device or BCROs for both mixed-mode and broadcast devices.

Figure 8 shows the key hierarchy for the case of a service-based subscription.



NOTE DRD – Device registration data: device-assigned keys during registration; see 5.4.5 and 5.4.6.

Figure 8 – 4-layer key hierarchy – Use of SEK only

5.4.2.2 Pay-per-view-based purchase and service-based subscription

If content is made available both via a service subscription and via a pay-per-view-based purchase then the TEK shall be encrypted with the PEK:

$$E\{PEK\}(TEK)$$

Devices that do not have a service-based subscription to that service can acquire the entitlement for a specific pay-per-view event. The RO for that pay-per-view event shall contain a PEK. This PEK can be used to decrypt the TEK:

$$TEK = D\{PEK\}(E\{PEK\}(TEK))$$

To allow devices with a service-based subscription to access the service as well, the PEK encrypted with the SEK is also carried in the key stream message. Therefore, the KSM carries

$$E\{SEK\}(PEK)$$

and

$$E\{PEK\}(TEK)$$

In order to decrypt the TEK given only the SEK, the device has to do the following decryption:

$$TEK = D\{PEK\}(E\{PEK\}(TEK))$$

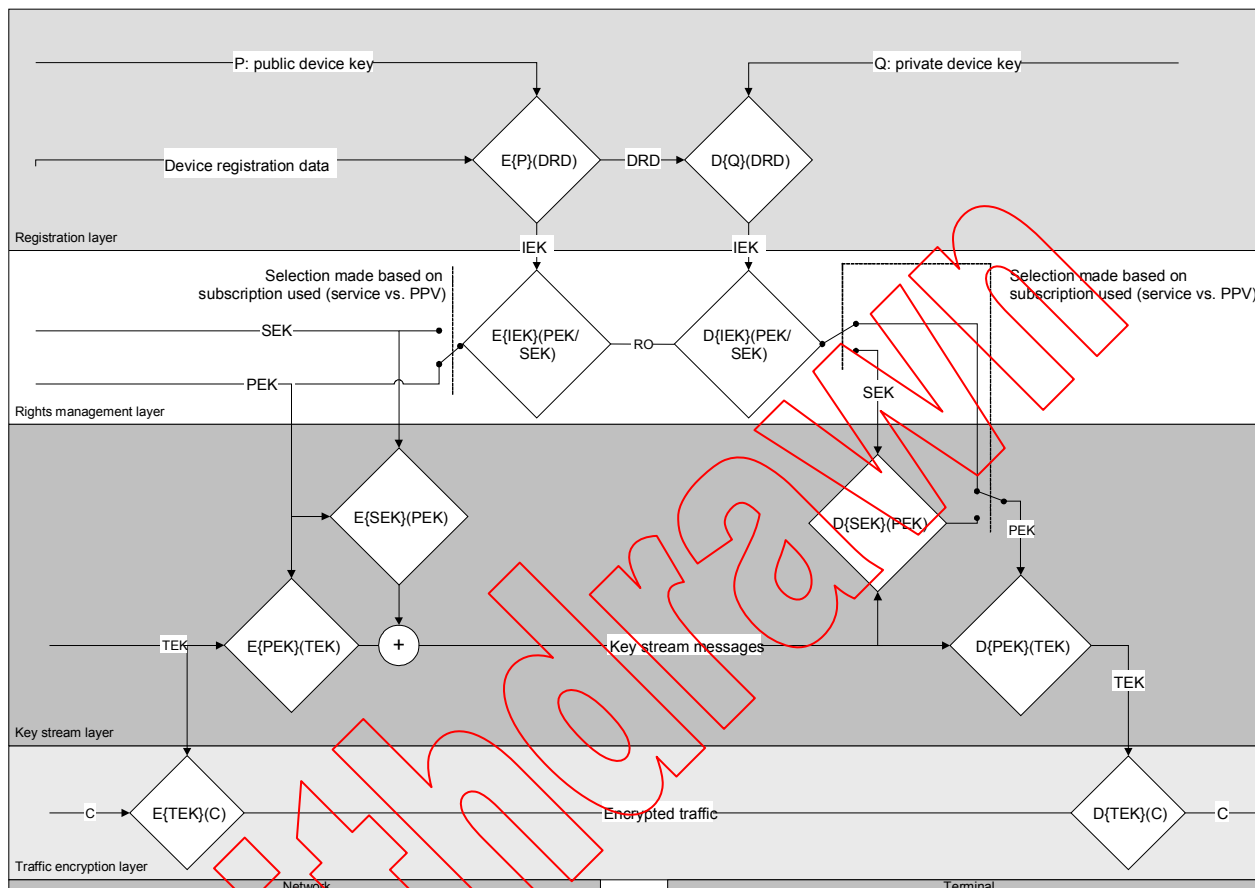
with

$$PEK = D\{SEK\}(E\{SEK\}(PEK))$$

hence

$$\text{TEK} = D\{D\{\text{SEK}\}(E\{\text{SEK}\}(\text{PEK}))\}(E\{\text{PEK}\}(\text{TEK}))$$

The lifetime of a PEK is expected to last only for the duration of a specific pay-per-view event while the SEK is expected to last for a longer period.



NOTE DRD – Device registration data: device-assigned keys during registration; see 5.4.5 and 5.4.6.

Figure 9 – 4-layer key hierarchy – Use of PEK and SEK

Figure 9 shows the four-layer key hierarchy in the case of service subscription and pay-per-view.

5.4.2.3 Pay-per-view-based consumption

If content can be consumed on a pay-per-view-only basis, that means that the content is not available via a service subscription, then the TEK may be encrypted with a PEK or the TEK may be encrypted with a SEK. Both PEK and SEK are interchangeable in this case.

5.4.3 Keys on the rights management layer (interactive mode)

If a rights object containing the SEK or PEK is delivered via an interactivity channel, the rights encryption key is used to decrypt the SEK/PEK. OMA-ERP-DRM-V2_0-20060303-A specifies how a device can obtain and use a rights encryption key. If the RO contains a CEK, it shall be processed according to OMA-ERP-DRM-V2_0-20060303-A and is beyond the scope of this standard.

5.4.4 Keys on the rights management layer (broadcast mode)

The SEK and PEK are transmitted to the device on the rights management layer as part of a BCRO.

The keys used to encrypt and decrypt the SEK or PEK depend on the addressing mode of the BCRO (see 5.5.2). The term "inferred encryption key" (IEK) is used to indicate the key used to en-/decrypt the SEK/PEK without specifying which exact key is used.

- **RO addressed to a unique device**

In the case where an RO is addressed to a unique device, the IEK used to encrypt the SEK or PEK shall be the unique device key (UDK) that was delivered during device registration.

- **RO addressed to a subscriber group (subset of unique group)**

In the case where an RO is addressed to a subset of a unique group (subscriber group), the IEK shall be deduced from the subscriber group keys (SGKs) by use of zero message broadcast encryption. See 5.5.3 for an explanation of the zero message broadcast encryption concept. See Clause A.7 for an explanation of how the IEK is deduced given the bit access mask and the SGKs.

- **RO addressed to a unique group**

In the case where an RO is addressed to all devices in a unique group, the IEK used to encrypt the SEK or PEK shall be the unique group key (UGK).

- **RO addressed to a domain**

In the case where an RO is addressed to a domain, the IEK used to encrypt the SEK or PEK shall be the broadcast domain key (BDK) that was delivered during device registration.

- **RO containing a CEK**

In the case where an RO is for an OMA DRM 2.0 content format (for example, a DCF), the asset shall carry a CEK object and an additional cipher value. Decryption of the key material is defined by OMA-ERP-DRM-V2_0-20060303-A.

5.4.5 Keys on the registration layer (interactive mode)

This is according to OMA-ERP-DRM-V2_0-20060303-A and is beyond the scope of this standard.

5.4.6 Keys on the registration layer (broadcast mode)

The registration layer delivers the keys used for the broadcast mode of operation. There are several keys used for authentication and decryption purposes.

Table 2 – Keyset in the registration data

Name of key	Description	Remark
UGK	unique_group_key	
SGK	subscriber_group_key	Used for zero message broadcast
BDK	broadcast_domain_key	Used for domains
UDK	unique_device_key	
RIAK	ri_authentication_key	Used for authentication
UDF	unique_device_filter	Eurocrypt address, not a key
SBDF	shortform_broadcast_domain_filter	domain_id address, not a key
LBDF	longform_broadcast_domain_filter	domain_id address, not a key
TDK	token_delivery_key	Used for token delivery, not for registration

The keyset itself is delivered to the device in a protected format as part of the device registration data (see 9.2.2.7.2 for details).

The RI generates a session key (SK) to protect the keyset_block (UGK, SGK1..n, UDK, BDK, RIAK, UDF, SBDF, LBDF and/or TDK), which carries the keyset specified in Table 2 above.

$$\text{encrypted_keyset_block} = E_{\{SK\}}(\text{keyset_block})$$

The RI encrypts the SK and the encrypted_keyset_block (together called the SK + encrypted_keyset_block) into a sessionkey_block, such that

$$\text{sessionkey_block} = E_{\{DP\}}(\text{SK} + \text{encrypted_keyset_block})$$

where the sessionkey_block is encrypted with the public key of the device (DP).

If the keyset_block does not fit into the size of the sessionkey_block, the remainder is kept as surplus_block. See 9.2.2.7.2.2 for details.

The complete message (header, sessionkey_block and optional surplus_block) is protected by a single source authenticity check, such that:

$$\text{signature_block} = A_{\{RIQ\}}(\text{message})$$

where the RIQ is the private key of the RI.

Upon reception, the device follows the rules specified above in reverse order:

$$V_{\{RIP\}}(\text{signature_block})$$

$$\text{SK} + \text{encrypted_keyset_block} = D_{\{DQ\}}(\text{sessionkey_block})$$

$$\text{keyset_block} = D_{\{SK\}}(\text{encrypted_keyset_block})$$

where the signature_block is verified with the RI public key (RIP).

The encrypted sessionkey_block contains the session key (SK) plus encrypted_keyset_block (together called the SK + encrypted_keyset_block) and is decrypted with the private key of the device (DQ).

If the surplus_block is present, it is concatenated to the keyset_block from the sessionkey_block. See 9.2.2.7.2.2 for details.

The encrypted_keyset_block, decrypted with the session key (SK), produces the keyset_block, containing the keyset (UGK, SGK, UDK, RIAK, UDF), which never leaves the DRM agent.

The notation HMAC_SHA1{k}(s) is used to denote the computation of HMAC, see IETF RFC 2104, with SHA1, see FIPS PUB 180-2:2002, as the hash function keyed by the key 'k' over the string 's'. HMAC_SHA1_128{k}(s) is used to denote the 128 most significant bits of HMAC_SHA1{k}(s) output.

A key IEK is "derived" from the UGK, SGK, UDK or BDK to decrypt the BCRO, such that

$$\text{IEK} = \text{HMAC_SHA1_128}\{\text{UGK}\}(\text{salt})$$

or

$$\text{IEK} = \text{HMAC_SHA1_128}\{\text{NK}_i \parallel \dots \parallel \text{NK}_j\}(\text{salt})$$

where the NKs are NK keys ordered according to the index (such that $i < j$) that are required for creating the key for the desired group. The keys NK are obtained using the scheme specified in 5.5.3. See 5.5.5.3 and A.7.

or

$$\text{IEK} = \text{HMAC_SHA1_128}\{\text{UDK}\}(\text{salt})$$

or

$$\text{IEK} = \text{HMAC_SHA1_128}\{\text{BDK}\}(\text{salt})$$

The IEK is used to decrypt the part of the BCRO containing key material, which carries CEK or SEK and/or PEK. The 'salt' parameter is the BCI value in the asset structure of the BCRO. The BCI value from the first asset structure in a BCRO shall be used for all assets in a BCRO structure.

Withdrawn

5.4.7 Authentication overview

Figure 10 explains the authentication "hierarchy" of the system.

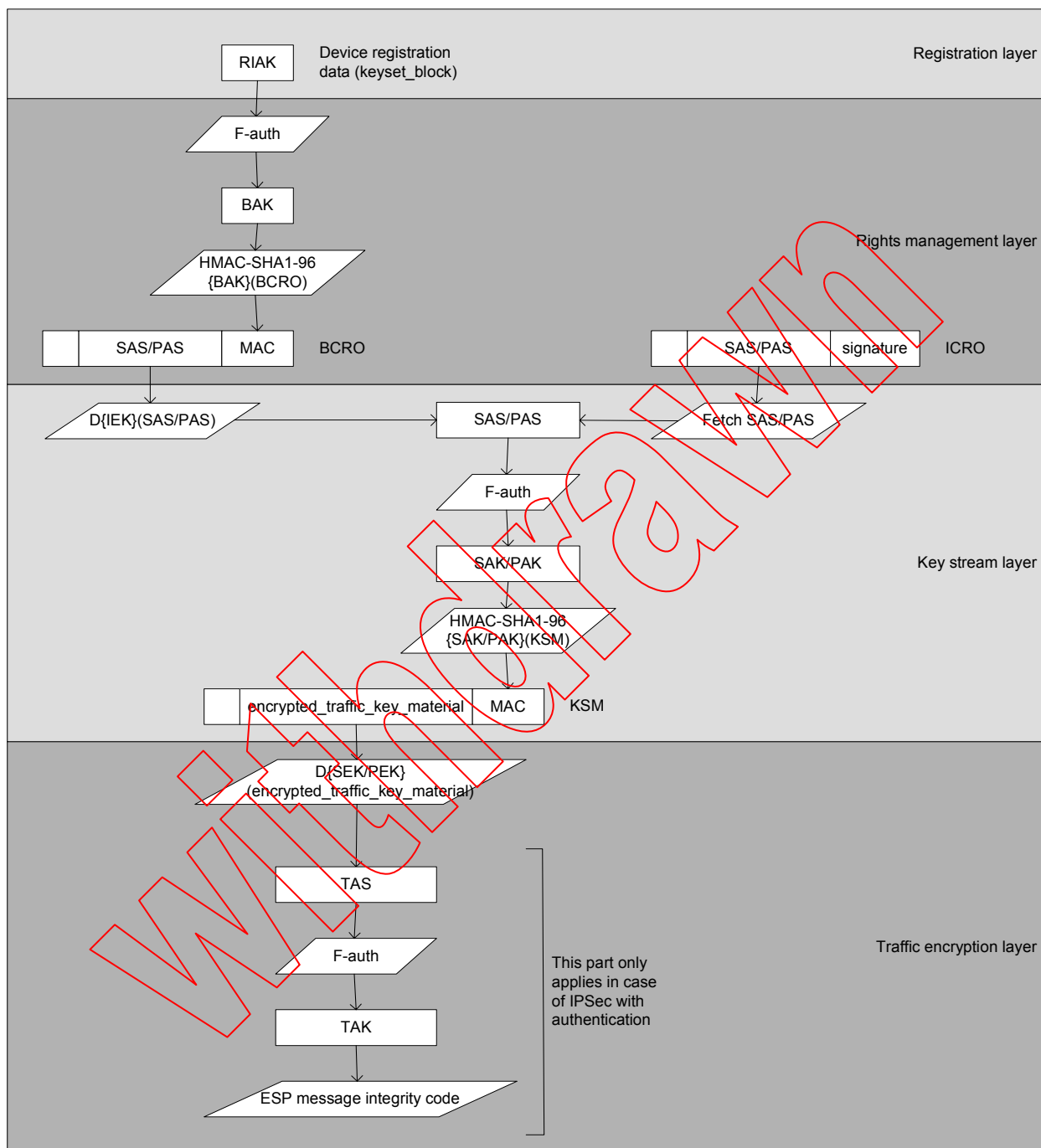


Figure 10 – Authentication hierarchy

5.4.7.1 Authentication keys on the traffic layer

When IPSec is used with authentication, the message shall be verifiable by the ESP integrity code. This shall be done by means of the traffic authentication key (TAK), which is derived from the traffic authentication seed (TAS) (see A.8.1).

5.4.7.2 Authentication keys on the key stream layer

The KSM shall be authenticated and the integrity of the message shall be verified. This shall be done by means of the programme authentication key (PAK) and/or the service authentication key (SAK), which are derived from the programme authentication seed (PAS) and the service authentication seed (SAS), which are delivered as part of the RO (see A.8.2).

5.4.7.3 Authentication keys on the rights management layer (broadcast mode)

The BCRO shall be authenticated and the integrity of the message shall be verified. This shall be done by means of the BCRO authentication key (BAK), which is derived from the RI authentication key (RIAK), which is delivered during registration (see A.8.3).

5.4.7.4 Authentication keys on the registration layer (broadcast mode)

The RI authentication key (RIAK) shall be delivered during registration as part of the device_registration_response(). See 9.2.2.4 for details.

5.5 Deployment for broadcast mode of operation

5.5.1 Concept of Domains –Interactive and broadcast domains

Content in OMA DRM 2.0 can be bound to a device or to a domain; see OMA-ERP-DRM-V2_0-20060303-A. In this standard, we refer to a domain as specified by OMA-ERP-DRM-V2_0-20060303-A as an interactive domain.

A domain in OMA-ERP-DRM-V2_0-20060303-A is a group of one or more devices that share a common secret, the so-called domain key. In the case of content that is bound to a domain, the content encryption key of that content as stored in the RO associated with that content is encrypted with the domain key of that domain. A device that receives an RO that is bound to a domain of which it is a member can freely pass that RO to other devices belonging to the same domain. The other devices in the same domain can then access that content as allowed by the RO.

OMA-ERP-DRM-V2_0-20060303-A defines protocols with which a device can join and leave a domain: the ROAP join domain protocol and the ROAP leave domain protocol. In order to use domain keys, the device shall have joined the corresponding domain. The equivalents for these protocols in the case that there is no interactivity channel are defined in 9.2.3.

The equivalent of the interactive domain in case there is no interactivity channel is the broadcast domain. In the BCRO, there is a facility to indicate that the BCRO is intended for a broadcast domain, using the address_mode. If the address_mode is set to "domain", the domain key is used for the encryption of the key material in the BCRO. Furthermore, if the address_mode is set to "domain", the domain_id is created by concatenating the address_field with the domain_id_extension.

NOTE While the domain ID and domain key may be the same in the case of the interactive and broadcast domain, the content for broadcast domains with BCROs is not interoperable with content for interactive domains with ICROs.

5.5.2 Addressing (group/subset/device/domain)

The registration data supports four methods of addressing devices, as explained in Figure 11.

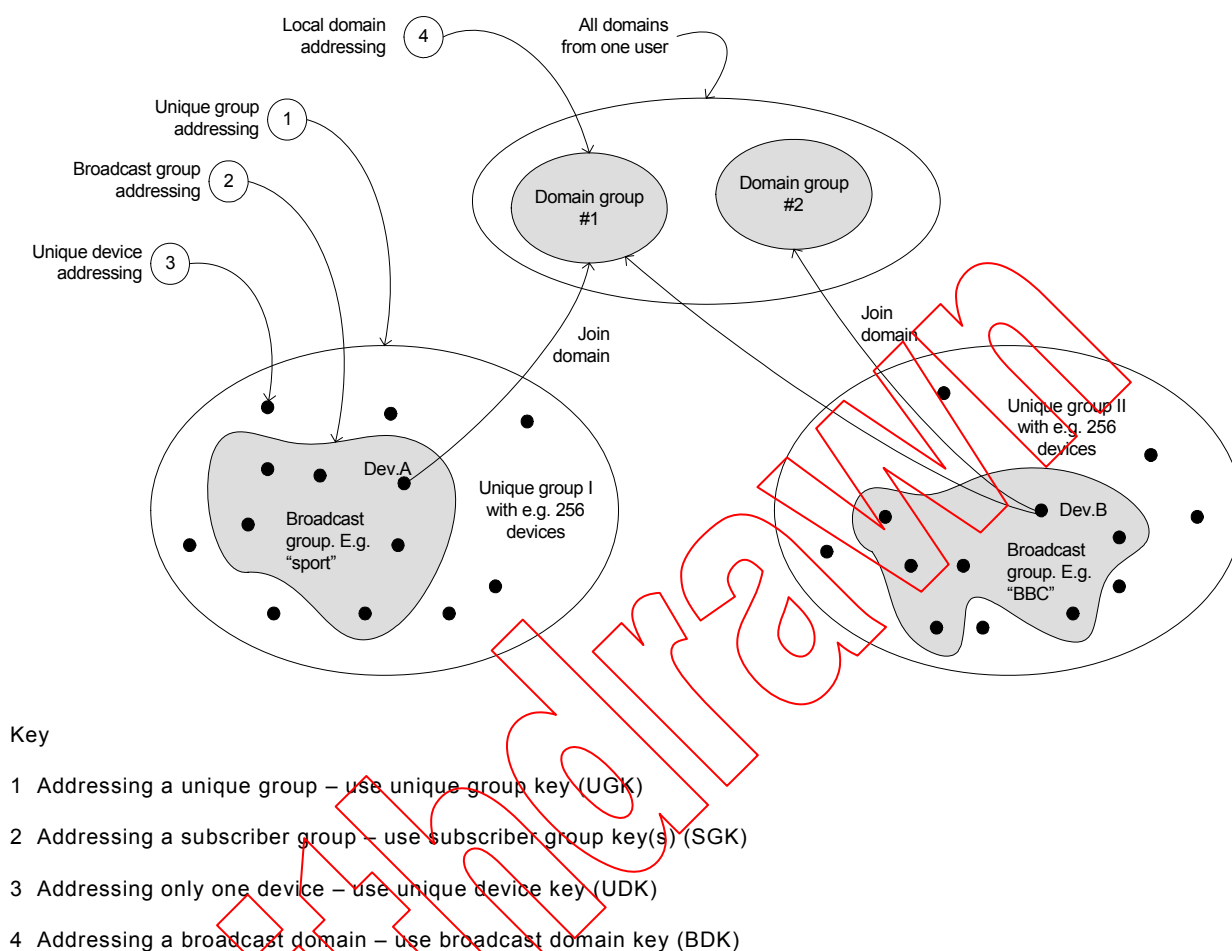


Figure 11 – Explaining the concept of addressing

A unique group contains all the devices in a group. A subscriber group can be smaller than, or as large as, the unique group. Alternatively, a device can be addressed via a (broadcast) domain group. A unique device can be part of a unique group and/or a subscriber group and/or a broadcast domain. One or more unique groups form the population of devices. In this example, the group size is 256 devices. Group sizes of 256 and 512 are supported, as these are acceptable group sizes when it should be needed to revoke devices. Using a larger group size is not supported because of the fact that eventual revocation of such a group easily concerns too many devices.

The following subclauses specify the relationship between the registration data and the broadcast rights object. The registration data is sent to the device after successful registration of the device. At a later stage, the device can receive a BCRO as a means to obtain the content encryption key, which in turn is used to decrypt the encrypted AV content. The content key may carry the SEK and/or PEK. The RI encrypts the content key with an inferred encryption key (IEK). The following subclauses specify the different addressing modes, how the message is filtered and what type of IEK will be used by the device to obtain the content key.

A device supporting broadcast mode of operation shall support all four addressing modes. The network operator can choose to send registration data with a keyset of UGK and/or SGK and/or UDK and/or BDK to the device at registration time.

See 5.4 for the general overview of the process used to construct the IEK.

5.5.2.1 Addressing the unique group

To access the whole group, the following (oversimplified) BCRO is used (see Figure 12).

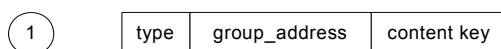


Figure 12 – (Oversimplified) group BCRO

- The `group_address` was delivered with the registration data and is used to filter for the message (see 9.2.2.7 for details).
- The content key (which can carry the SEK and/or PEK) is encrypted with an inferred entitlement key (IEK). In this case, the `unique_group_key` (UGK) is used as the IEK. The UGK used by the RI is identical to the key that was delivered with the registration data sent to the device (see 9.2.2.7 for details).
- All the devices in the group can use the content key.

5.5.2.2 Addressing a subscriber group

The subscriber group is a privileged subset of the unique group. Two methods are available to address the subscriber group, but either one can be used.

- At registration, the registration data delivers a set of `subscriber_group_keys` (SGK) to the Device. By using zero message broadcast encryption (see 5.5.3), an inferred encryption key (IEK) can be constructed from the SGKs sent to the device. The RI uses this IEK to encrypt the content key and only the devices with the matching set of SGKs on board can construct the same IEK.
- For reasons of completeness, it is mentioned that is also possible to deliver no SGKs with the registration data. With 0 (zero) SGKs, it is, of course, not possible to deduce an IEK. In this case, a unique device addressing with a `unique_device_key` (UDK) as the IEK is used. See 5.5.2.3 for more details.

NOTE It is inefficient for large populations to use unique addressing instead of (broadcast) group addressing, since it quickly consumes a considerable amount of bandwidth.

To access the subscriber group, the following (oversimplified) BCRO is used (see Figure 13).

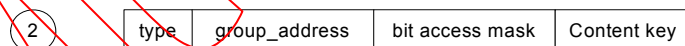


Figure 13 – (Oversimplified) subscriber group BCRO

For both methods, the `group_address` was delivered with the registration data and is used to filter for the message.

- The `group_address` is part of the `unique_device_filter` (UDF) address that was sent with the registration data to the device and is used to filter for the message (see 9.2.2.7 for details).
- The Eurocrypt-style bit access mask, see EN 50094:1992, prescribes which group members are "entitled" to use the content key (which can carry the SEK and/or PEK). This bit mask indicates which group members of the subscriber group can deduce the broadcast key from the zero message broadcast keys in the device.
- The device can construct the inferred encryption key (IEK) from the SGKs that were delivered to the device. The SGKs used in this process belong to the same RI context as the BCRO.
- Only members of the subscriber group can use the content key. If a member of the group succeeds in constructing the IEK, that member can decrypt the content key. Any group member that tries to deduce the IEK but does not have the appropriate (zero message) SGK on board is unable to deduce the IEK to decrypt the content key.