

ETSI TS 103 197 V1.5.1 (2008-10)

Technical Specification

Digital Video Broadcasting (DVB); Head-end implementation of DVB SimulCrypt

European Broadcasting Union



Union Européenne de Radio-Télévision



Reference

RTS/JTC-DVB-231

Keywords

broadcasting, digital, DVB, interface, video

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2008.

© European Broadcasting Union 2008.

All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM, **TIPHON**TM, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Contents

Intellectual Property Rights	12
Foreword.....	12
1 Scope	13
1.1 Common scrambling algorithm	13
1.2 Language	13
2 References	13
2.1 Normative references	14
2.2 Informative references.....	15
3 Definitions and abbreviations.....	16
3.1 Definitions	16
3.2 Abbreviations	18
4 Architecture.....	19
4.1 System architecture	19
4.1.1 Host Head-end components	20
4.1.2 Simulcrypt CA components.....	20
4.1.3 Simulcrypt Integrated Management Framework (SIMF).....	21
4.1.4 Multiplexer Redundancy.....	21
4.2 Description of Components.....	21
4.2.1 Event Information Scheduler (EIS)	21
4.2.2 Simulcrypt Synchronizer (SCS).....	21
4.2.3 ECM Generator (ECMG).....	21
4.2.4 EMM Generator (EMMG).....	22
4.2.5 Private Data Generator (PDG).....	22
4.2.6 Service Information Generator (SIG)	22
4.2.7 Program Specific Information Generator (PSIG)	22
4.2.8 Custom Service Information Generator (CSIG)	22
4.2.9 Custom Program Specific Information Generator (CPSIG)	22
4.2.10 Multiplexer Configuration (MUXCONFIG)	22
4.2.11 Multiplexer (MUX).....	23
4.2.12 Scrambler (SCR).....	23
4.2.13 Control Word Generator (CWG)	23
4.2.14 Network Management System (NMS).....	23
4.2.15 SIMF agent	23
4.2.16 Access Criteria Generator (ACG).....	23
4.3 Description of interfaces	23
4.3.1 ECMG \leftrightarrow SCS	23
4.3.2 EMMG \leftrightarrow MUX	23
4.3.3 PDG \leftrightarrow MUX.....	23
4.3.4 Custom (P)SI Generator \leftrightarrow (P)SI Generator	24
4.3.5 EIS \leftrightarrow SIG.....	24
4.3.6 (P)SI Generator \leftrightarrow MUX.....	24
4.3.7 EIS \leftrightarrow MUXCONFIG	24
4.3.8 MUXCONFIG \leftrightarrow PSIG	24
4.3.9 MUXCONFIG \leftrightarrow SCS	24
4.3.10 MUX \leftrightarrow SCR	24
4.3.11 SCR onward.....	24
4.3.12 SCS \leftrightarrow MUX.....	24
4.3.13 SCS \leftrightarrow SCR	24
4.3.14 SCS \leftrightarrow CWG.....	24
4.3.15 EIS \leftrightarrow SCS	24
4.3.16 ACG \leftrightarrow EIS.....	25
4.3.17 NMS Component \leftrightarrow SIMF Agent.....	25
4.3.18 SIMCOMP \leftrightarrow MUXCONFIG.....	25

4.3.19	Mandatory or optional characteristics of Simulcrypt interfaces	25
4.4	Protocol types	26
4.4.1	Connection-oriented TLV protocols	26
4.4.2	Connection oriented XML protocols	29
4.4.3	SIMF-based protocols.....	29
5	ECMG \leftrightarrow SCS interface	29
5.1	Interface principles	29
5.1.1	Channel and Stream specific messages.....	29
5.1.2	Channel establishment	30
5.1.3	Stream establishment	30
5.1.4	Stream closure	30
5.1.5	Channel closure	30
5.1.6	Channel/Stream testing and status	30
5.1.7	Unexpected communication loss	31
5.1.8	Handling data inconsistencies.....	31
5.2	Parameter_type values.....	31
5.3	Parameter semantics	32
5.4	Channel specific Messages.....	34
5.4.1	Channel_setup message: ECMG \leftarrow SCS.....	34
5.4.2	Channel_test message: ECMG \leftrightarrow SCS	34
5.4.3	Channel_status message: ECMG \leftrightarrow SCS.....	34
5.4.4	Channel_close message: ECMG \leftarrow SCS.....	35
5.4.5	Channel_error message: ECMG \leftrightarrow SCS	35
5.5	Stream specific messages	35
5.5.1	Stream_setup message: ECMG \leftarrow SCS.....	35
5.5.2	Stream_test message: ECMG \leftrightarrow SCS	35
5.5.3	Stream_status message: ECMG \leftrightarrow SCS.....	35
5.5.4	Stream_close_request message: ECMG \leftarrow SCS	36
5.5.5	Stream_close_response message: ECMG \Rightarrow SCS	36
5.5.6	Stream_error message: ECMG \leftrightarrow SCS	36
5.5.7	CW_provision message: ECMG \leftarrow SCS.....	36
5.5.8	ECM_response message: ECMG \Rightarrow SCS.....	38
5.6	Error status	38
5.7	Security in ECMG \leftrightarrow SCS protocol.....	39
6	EMMG \leftrightarrow MUX and PDG \leftrightarrow MUX interfaces	39
6.1	Transport layer protocols for EMMG/PDG \leftrightarrow MUX interfaces.....	39
6.2	TCP-based protocol.....	40
6.2.1	Interface principles	40
6.2.1.1	Channel and Stream specific messages.....	40
6.2.1.2	Channel establishment	40
6.2.1.3	Stream establishment	40
6.2.1.4	Bandwidth allocation	41
6.2.1.5	Stream closure.....	41
6.2.1.6	Channel closure.....	41
6.2.1.7	Channel/Stream testing and status.....	41
6.2.1.8	Unexpected connection loss	41
6.2.1.9	Handling data inconsistencies	41
6.2.2	Parameter Type Values	42
6.2.3	Parameter semantics	42
6.2.4	Channel specific messages.....	43
6.2.4.1	Channel_setup message: EMMG/PDG \Rightarrow MUX.....	43
6.2.4.2	Channel_test message: EMMG/PDG \leftrightarrow MUX	43
6.2.4.3	Channel_status message: EMMG/PDG \leftrightarrow MUX.....	43
6.2.4.4	Channel_close message: EMMG/PDG \Rightarrow MUX.....	44
6.2.4.5	Channel_error message: EMMG/PDG \leftrightarrow MUX.....	44
6.2.5	Stream specific messages.....	44
6.2.5.1	Stream_setup message: EMMG/PDG \Rightarrow MUX.....	44
6.2.5.2	Stream_test message: EMMG/PDG \leftrightarrow MUX	44
6.2.5.3	Stream_status message: EMMG/PDG \leftrightarrow MUX.....	44

6.2.5.4	Stream_close_request message: EMMG/PDG ⇒ MUX.....	45
6.2.5.5	Stream_close_response message: EMMG/PDG ⇐ MUX	45
6.2.5.6	Stream_error message: EMMG/PDG ⇔ MUX	45
6.2.5.7	Stream_BW_request message: EMMG/PDG ⇒ MUX	45
6.2.5.8	Stream_BW_allocation message: EMMG/PDG ⇐ MUX	46
6.2.5.9	Data_provision message: EMMG/PDG ⇒ MUX	46
6.2.6	Error status	46
6.3	UDP-based protocol	47
6.3.1	Interface principles	47
6.3.1.1	Data_provision message: EMMG/PDG ⇒ MUX	48
6.3.1.2	Channel and stream configuration messages.....	49
6.3.2	Bandwidth management	49
7	Network management.....	49
7.1	SIMF overview.....	49
7.1.1	Introduction to the Common Information Model (CIM)	50
7.1.2	SIMF specialization options	51
7.2	Common Information Model (CIM).....	51
7.2.1	Object Containment Hierarchy	52
7.2.2	MIB II.....	54
7.2.3	Concurrency control	54
7.2.4	Simulcrypt Events Module (SEM).....	55
7.2.4.1	Event Group	57
7.2.4.2	Event Forwarding Discriminator (EFD) Group	58
7.2.4.3	Event Notification Group	59
7.2.4.4	Conformance requirements	60
7.2.5	Simulcrypt Logs Module (SLM)	62
7.2.5.1	Log Control Group.....	64
7.2.5.2	Logs Group	66
7.2.5.3	Conformance Requirements.....	67
7.3	CAS component monitoring and configuration.....	69
7.3.1	Ident Group.....	71
7.3.2	ECM Generator Group.....	71
7.3.3	EMMG/PDG Group.....	73
7.3.4	C(P)SIG Group	76
7.3.5	Conformance Requirements.....	79
8	C(P)SIG ⇔ (P)SIG interface.....	79
8.1	Overview and Scope.....	79
8.1.1	Note on commercial agreements.....	80
8.1.2	Note on the PDG ⇔ MUX Interface	80
8.2	Application protocol model.....	81
8.2.1	Overview of the C(P)SIG ⇔ (P)SIG Application Protocol.....	81
8.2.2	Configurations and Topologies.....	81
8.2.3	Trigger Transaction Type	82
8.2.4	Table Provisioning Transaction Type	84
8.2.5	Descriptor Insertion Transaction Type	85
8.2.6	Service Change Transaction Type	87
8.2.7	Flow PID Provisioning Transaction Type	88
8.2.8	Implementation of the C(P)SIG ⇔ (P)SIG protocol	91
8.3	Connection-oriented protocol.....	91
8.3.1	Overview of the C(P)SIG ⇔ (P)SIG connection-oriented protocol	91
8.3.1.1	Principles.....	91
8.3.1.2	Channels.....	92
8.3.1.2.1	Definition and types	92
8.3.1.2.2	Channel establishment.....	92
8.3.1.3	Streams.....	92
8.3.1.3.1	Definition.....	92
8.3.1.3.2	Stream establishment.....	93
8.3.1.4	C(P)SIG ⇔ (P)SIG message lists	93
8.3.1.5	Protocol state machines definition	94
8.3.1.6	Channel state machine.....	94

8.3.1.6.1	Channel Not Open	95
8.3.1.6.2	Channel Setting Up.....	95
8.3.1.6.3	Channel Open	95
8.3.1.6.4	Channel In Error.....	96
8.3.1.7	Stream state machine.....	96
8.3.1.7.1	Stream Not Open	98
8.3.1.7.2	Stream Setting Up.....	98
8.3.1.7.3	Stream Open	98
8.3.1.7.4	Stream Trigger Enabling	99
8.3.1.7.5	Stream Trigger-Enabled	99
8.3.1.7.6	Stream In Error	100
8.3.1.7.7	Stream Closing	100
8.3.1.8	Summary of messages permissible in each state	100
8.3.2	C(P)SIG \leftrightarrow (P)SIG message syntax and semantics.....	102
8.3.2.1	List of message parameters for the C(P)SIG \leftrightarrow (P)SIG protocol	102
8.3.2.2	Parameter semantics	103
8.3.3	Channel-level messages	107
8.3.3.1	Channel_setup message: C(P)SIG \leftarrow (P)SIG	107
8.3.3.2	Channel_status message: C(P)SIG \leftrightarrow (P)SIG	107
8.3.3.3	Channel_test message: C(P)SIG \leftrightarrow (P)SIG	108
8.3.3.4	Channel_close message: C(P)SIG \leftarrow (P)SIG.....	108
8.3.3.5	Channel_error message: C(P)SIG \leftrightarrow (P)SIG.....	108
8.3.4	Stream-level messages	109
8.3.4.1	stream_setup message: C(P)SIG \leftarrow (P)SIG.....	109
8.3.4.2	Stream_status message: C(P)SIG \leftrightarrow (P)SIG	109
8.3.4.3	Stream_test message: C(P)SIG \leftrightarrow (P)SIG.....	110
8.3.4.4	Stream_close message: C(P)SIG \leftarrow (P)SIG.....	110
8.3.4.5	Stream_close_request message: C(P)SIG \Rightarrow (P)SIG	110
8.3.4.6	Stream_close_response message: C(P)SIG \leftarrow (P)SIG.....	110
8.3.4.7	Stream_error message: C(P)SIG \leftrightarrow (P)SIG.....	111
8.3.4.8	Stream_service_change message: C(P)SIG \leftarrow (P)SIG	111
8.3.4.9	Stream_trigger_enable_request message: C(P)SIG \Rightarrow (P)SIG	111
8.3.4.10	Stream_trigger_enable_response message: C(P)SIG \leftarrow (P)SIG.....	112
8.3.4.11	Trigger message: C(P)SIG \leftarrow (P)SIG	112
8.3.4.12	Table_request message: C(P)SIG \Rightarrow (P)SIG	113
8.3.4.13	Table_response message: C(P)SIG \leftarrow (P)SIG	114
8.3.4.14	Descriptor_insert_request message: C(P)SIG \Rightarrow (P)SIG.....	114
8.3.4.15	Descriptor_insert_response message: C(P)SIG \leftarrow (P)SIG	115
8.3.4.16	PID_provision_request message: C(P)SIG \Rightarrow (P)SIG	116
8.3.4.17	PID_provision_response message: C(P)SIG \leftarrow (P)SIG.....	116
8.3.5	Error status and error information.....	117
8.4	SIMF-based protocol.....	118
8.4.1	Operations Reference Points (ORPs).....	118
8.4.2	Application of ORPs to the C(P)SIG \leftrightarrow (P)SIG Interface.....	119
8.4.2.1	ECM/Event/Flow Change Triggering	120
8.4.2.2	(P)SI Table Provisioning.....	120
8.4.2.3	(P)SI Descriptor Insertion	120
8.4.2.4	Transport Stream Service Changes	121
8.4.2.5	PID Provisioning.....	121
8.4.3	SIM (P)SIG Group Specification.....	121
8.4.3.1	Information Table	121
8.4.3.2	Configuration Table	122
8.4.3.3	ECM Trigger Table.....	122
8.4.3.4	Flow PID Change Trigger Table.....	123
8.4.3.5	Event Trigger Table	124
8.4.3.6	PD Trigger Table	125
8.4.3.7	Descriptor Insert Table.....	126
8.4.3.8	Descriptor Insert Descriptor Table.....	128
8.4.3.9	Table Request Table.....	128
8.4.3.10	PID Provisioning Table.....	130

8.4.4	Conformance Requirements.....	130
9	(P)SIG \Leftrightarrow MUX interface	131
9.1	Overview	131
9.2	Interface principles	132
9.2.1	Description.....	132
9.2.1.1	Model of the interface (P)SIG \Leftrightarrow MUX with the carousel built in the MUX.....	132
9.2.1.2	Model of the interface (P)SIG \Leftrightarrow MUX with the carousel built in the (P)SIG.....	133
9.2.2	Channel and Stream specific messages.....	133
9.2.3	Channel establishment	134
9.2.4	Stream level protocol for the model with the carousel in the MUX	134
9.2.4.1	Stream establishment	134
9.2.4.2	Provision of the PSI/SI or private sections.....	135
9.2.4.3	Stream closure.....	135
9.2.5	Stream level protocol for the model with the carousel in the (P)SIG	135
9.2.5.1	Stream establishment	135
9.2.5.2	Bandwidth allocation	136
9.2.5.3	Stream closure.....	136
9.2.6	Channel closure	136
9.2.7	Channel/Stream testing and status	136
9.2.8	Unexpected communication loss	136
9.2.9	Handling data inconsistencies.....	136
9.2.10	Error management.....	137
9.3	Parameter_type values.....	137
9.4	Parameter semantics	137
9.5	Channel specific Messages.....	139
9.5.1	Channel_setup message: (P)SIG \Rightarrow MUX.....	139
9.5.2	channel_test message: (P)SIG \Leftrightarrow MUX	139
9.5.3	channel_status message: (P)SIG \Leftrightarrow MUX.....	139
9.5.4	channel_close message: (P)SIG \Rightarrow MUX.....	140
9.5.5	channel_error message: (P)SIG \Leftrightarrow MUX.....	140
9.6	Stream specific messages for both models	140
9.6.1	stream_setup message: (P)SIG \Rightarrow MUX	140
9.6.2	Stream_test message: (P)SIG \Leftrightarrow MUX	140
9.6.3	Stream_status message: (P)SIG \Leftrightarrow MUX.....	141
9.6.4	Stream_close_request message: (P)SIG \Rightarrow MUX	141
9.6.5	Stream_close_response message: (P)SIG \Leftarrow MUX.....	141
9.6.6	Stream_error message: (P)SIG \Leftrightarrow MUX.....	141
9.7	Specific messages for the model with the carousel in the MUX.....	142
9.7.1	CiM_stream_section_provision: (P)SIG \Rightarrow MUX.....	142
9.7.2	CiM_channel_reset: (P)SIG \Rightarrow MUX.....	142
9.8	Specific messages for the model with the carousel in the (P)SIG	143
9.8.1	CiP_Stream_BW_request message: (P)SIG \Rightarrow MUX	143
9.8.2	CiP_stream_BW_allocation message: (P)SIG \Leftarrow MUX.....	143
9.8.3	CiP_stream_data_provision message: (P)SIG \Rightarrow MUX.....	143
9.9	Error status	143
10	EIS \Leftrightarrow SCS Interface	144
10.1	Overview	144
10.2	Interface principles	145
10.2.1	Channel specific messages.....	145
10.2.2	Scrambling Control Group (SCG) specific messages	145
10.2.3	Channel establishment	146
10.2.4	Scrambling Control Group provisioning.....	146
10.2.5	Channel closure	146
10.2.6	Channel testing and status.....	146
10.2.7	Scrambling Control Group testing and status	147
10.2.8	Unexpected communication loss	147
10.2.9	Handling data inconsistencies.....	147
10.2.10	Error management.....	147
10.3	Parameter_type values.....	148

10.4	Parameter Semantics	148
10.5	Channel specific messages	150
10.5.1	channel_setup message: EIS \Rightarrow SCS	150
10.5.2	channel_test message: EIS \Leftrightarrow SCS.....	150
10.5.3	channel_status message: EIS \Leftrightarrow SCS	150
10.5.4	channel_close message: EIS \Rightarrow SCS	151
10.5.5	channel_reset message: EIS \Rightarrow SCS	151
10.5.6	channel_error message: EIS \Leftrightarrow SCS	151
10.6	SCG specific messages.....	152
10.6.1	SCG_provision message: EIS \Rightarrow SCS	152
10.6.2	SCG_test message: EIS \Rightarrow SCS	153
10.6.3	SCG_status message: EIS \Leftarrow SCS	154
10.6.3.1	Response to a provisioning message.....	154
10.6.3.2	Response to a test message	154
10.6.3.3	Management of the <i>SCG_nominal_CP_duration</i> parameter.....	154
10.6.4	SCG_list_request message: EIS \Rightarrow SCS.....	155
10.6.5	SCG_list_response message: EIS \Leftarrow SCS	155
10.6.6	SCG_error message: EIS \Leftarrow SCS	155
10.6.7	ECM_Group: CompoundTLV	155
10.7	Error status	156
11	ACG \Leftrightarrow EIS Interface	157
11.1	Overview	157
11.2	Scope	157
11.2.1	Role of the ACG	157
11.2.2	Role of the EIS.....	158
11.2.3	Dynamics of the ACG \Leftrightarrow EIS Interface	159
11.3	Interface Principles.....	160
11.3.1	General Principles.....	160
11.3.2	Channel Specific Messages.....	160
11.3.3	Messages for Access Criteria Creation and Modification.....	161
11.3.4	Channel Establishment	161
11.3.5	Channel Closure.....	161
11.3.6	Channel Testing and Status.....	161
11.3.7	Unexpected Communication Loss	161
11.3.8	Handling Data Inconsistencies.....	161
11.3.9	Handling Multiple AC Parameters in one AC Response	161
11.3.10	Handling AC Expiration Time.....	162
11.3.11	Asynchronous Access Criteria Change Request.....	162
11.3.12	Inserting Additional Information in the AC.....	163
11.3.13	Data Communications and Message Format	163
11.4	Interface Structure	163
11.5	Parameter Semantics	165
11.6	Parameter Types	167
11.7	Parameters Substitution.....	167
11.8	Channel Specific Messages	168
11.8.1	The <i>channel_setup</i> Message (EIS \Rightarrow ACG).....	168
11.8.2	The <i>channel_test</i> Message (EIS \Leftrightarrow ACG).....	169
11.8.3	The <i>channel_status</i> Message (EIS \Leftrightarrow ACG).....	169
11.8.4	The <i>channel_error</i> Message (EIS \Leftrightarrow ACG).....	170
11.8.5	The <i>channel_close</i> Message (EIS \Rightarrow ACG).....	170
11.9	Messages of Access Criteria Creation and Modification.....	170
11.9.1	The <i>AC_request</i> Message (EIS \Rightarrow ACG).....	170
11.9.2	The <i>AC_response</i> Message (EIS \Leftarrow ACG)	171
11.9.3	The <i>AC_interrupt</i> Message (EIS \Leftarrow ACG)	172
11.9.4	The <i>AC_error</i> Message (EIS \Leftarrow ACG)	172
11.10	Error Status.....	173
12	SIMCOMP \Leftrightarrow MUXCONFIG Interface.....	173
12.1	Overview	173
12.2	Interface Principles.....	174

12.2.1	System Diagram.....	174
12.2.2	Data Communications and Message Format	175
12.2.3	Message Groups.....	175
12.2.3.1	Communication channel messages.....	175
12.2.3.2	Transport resource mapping messages.....	175
12.2.4	Channel Establishment	176
12.2.5	Timeout and Retry	176
12.2.6	Channel closure	176
12.2.7	Channel testing and status.....	177
12.2.8	Handling data inconsistencies.....	177
12.3	Parameter Semantics	177
12.4	Interface Structure	179
12.5	Channel Specific Messages	179
12.5.1	The <i>channel_setup</i> message (SIMCOMP ⇔ MUXCONFIG).....	179
12.5.2	The <i>channel_status</i> message (SIMCOMP ⇔ MUXCONFIG).....	180
12.5.3	The <i>channel_test</i> message (SIMCOMP ⇔ MUXCONFIG).....	181
12.5.4	The <i>channel_close</i> message (SIMCOMP ⇔ MUXCONFIG).....	182
12.5.5	The <i>channel_error</i> message (SIMCOMP ⇔ MUXCONFIG).....	182
12.6	Transport Resource Mapping Messages.....	183
12.6.1	The <i>TS_resource_discover</i> message (SIMCOMP ⇔ MUXCONFIG).....	183
12.6.2	The <i>TS_resource_request</i> message (SIMCOMP ⇔ MUXCONFIG).....	183
12.6.3	The <i>TS_resource_update</i> message (SIMCOMP ⇔ MUXCONFIG).....	184
13	Timing and Play-out Issues	186
13.1	Timing issues.....	186
13.2	Delay Start.....	187
13.3	Play-out Issues.....	188
13.3.1	ECMs	188
13.3.2	EMMs and Private Data.....	188
13.4	Crypto-Period Realignment.....	188
Annex A (normative): System Layering.....		190
A.1	Introduction	190
A.2	Physical Layer	190
A.3	Data Link Layer	190
A.4	Network Layer.....	190
A.5	Transport Layer	190
A.6	Session Layer	190
A.7	System Layering Overview/Communications Protocol stack.....	191
A.8	TCP or UDP Connection Establishment	192
Annex B (informative): SCS Coexistence.....		193
B.1	Introduction	193
B.2	Example scenario	193
Annex C (informative): Control word generation and testing		194
C.1	Introduction	194
C.2	Background	194
C.3	Generation	194
C.4	Control word randomness verification testing	195
C.4.1	1/0 bias	195
C.4.2	Autocorrelation.....	195
C.5	Testing locations	195

Annex D (informative):	Security Method for the SCS \Leftrightarrow ECMG Interface	196
D.1	Algorithm Selection	196
D.2	Control Word processing.....	197
D.3	Key Management	197
D.3.1	Key Generation/Distribution	197
D.3.2	Selection	198
D.3.3	Key Pointer Distribution	199
D.3.4	Fixed Key Mode.....	199
D.4	Encryption Function Toggling	200
Annex E (normative):	Summary of Requirements for C(P)SIG \Leftrightarrow (P)SIG interface	201
E.1	Head-end system requirements	201
E.2	CAS's C(P)SIG requirements	202
Annex F (informative):	C(P)SIG\Leftrightarrow(P)SIG Connection-oriented Configuration Example	204
F.1	Head-end processes and configuration data	204
F.2	CAS processes and configuration data.....	205
F.3	Channels and configuration data	205
F.4	Streams and configuration data	206
Annex G (normative):	Transition Timing for EIS \Leftrightarrow SCS	208
Annex H (normative):	Crypto-period duration management by the SCS	211
H.1	<i>Nominal_CP_duration</i> in ECMG \Leftrightarrow SCS protocol	211
H.2	Management of the <i>recommended_CP_duration</i> value	211
Annex I (normative):	Standard compliance	213
I.1	Overview	213
I.2	General compliance scheme for connection-based protocols.....	214
I.3	Functional difference between V2 and V3 in ECMG \Leftrightarrow SCS protocol.....	215
I.4	Functional differences between V2 and V3 in EMMG \Leftrightarrow PDG protocol	215
I.5	Functional differences between V2 and V3 in C(P)SIG \Leftrightarrow (P)SIG protocol.....	215
I.6	SIMF.....	215
I.6.1	Functional differences between V2 and V3.....	215
I.6.2	Recommendation for SIMF compliance.....	215
I.7	Functional differences between V3 and V4 in EIS \Leftrightarrow SCS protocol.....	216
I.8	Functional differences between V3 and V4 in (P)SIG \Leftrightarrow MUX protocol	216
I.9	Functional differences between V4 and V5 in ECMG \Leftrightarrow SCS and EMMG \Leftrightarrow MUX protocols.....	216
Annex J (informative):	Use of DVB ASI for the PSIG \Leftrightarrow MUX interface	217
Annex K (normative):	ASN.1 MIBs description.....	218
K.1	SIM MIB	218
K.2	SEM MIB	256
K.3	SLM MIB	272
Annex L (normative):	SIMCOMP\LeftrightarrowMUXCONFIG XML Schema Definition	284

Annex M (normative):	ACG ↔ EIS XML Schema Definition	286
Annex N (normative):	ECMG ↔ SCS and EMMG ↔ MUX interfaces adaptations for use with IP Datacasting over DVB-H	289
N.1	Introduction	289
N.2	CP_CW_combination parameter in ECMG ↔ SCS	289
N.3	Section_TSpkt_flag parameter in ECMG ↔ SCS	290
N.4	Section_TSpkt_flag parameter in EMMG ↔ MUX	290
N.5	IPsec Traffic Authentication Key Derivation	290
Annex O (informative):	Bibliography	292
History	293

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://webapp.etsi.org/IPR/home.asp>).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by Joint Technical Committee (JTC) Broadcast of the European Broadcasting Union (EBU), Comité Européen de Normalisation ELECTrotechnique (CENELEC) and the European Telecommunications Standards Institute (ETSI).

NOTE: The EBU/ETSI JTC Broadcast was established in 1990 to co-ordinate the drafting of standards in the specific field of broadcasting and related fields. Since 1995 the JTC Broadcast became a tripartite body by including in the Memorandum of Understanding also CENELEC, which is responsible for the standardization of radio and television receivers. The EBU is a professional association of broadcasting organizations whose work includes the co-ordination of its members' activities in the technical, legal, programme-making and programme-exchange domains. The EBU has active members in about 60 countries in the European broadcasting area; its headquarters is in Geneva.

European Broadcasting Union
CH-1218 GRAND SACONNEX (Geneva)
Switzerland
Tel: +41 22 717 21 11
Fax: +41 22 717 24 81

Founded in September 1993, the DVB Project is a market-led consortium of public and private sector organizations in the television industry. Its aim is to establish the framework for the introduction of MPEG-2 based digital television services. Now comprising over 200 organizations from more than 25 countries around the world, DVB fosters market-led systems, which meet the real needs, and economic circumstances, of the consumer electronics and the broadcast industry.

1 Scope

The present document of DVB-Simulcrypt addresses the requirements for interoperability between two or more conditional access systems at a head-end. It specifies the system architecture, timing relationships, messaging structures, extended interoperability and control.

The components within the system architecture represent functional units. The boundaries between physical units are not required to match the boundaries between functional units. It is possible that the SCS could be in the MUX or the SCS and MUX could be built independently. Neither architecture is mandated.

1.1 Common scrambling algorithm

The DVB-Simulcrypt group has looked at issues relating to the concepts of the common scrambling algorithm, within the DVB-Simulcrypt environment.

The DVB-Simulcrypt system is based on the concept of a shared scrambling and descrambling method. The group has looked at the possible constraints, which the DVB-Simulcrypt architecture might impose on the use of such a shared scrambling and descrambling method. No problems were noted.

1.2 Language

The word "shall" is used in a normative statement that can be verified and is mandatory. The word "should" is used in the context of a recommendation or a statement that cannot be verified or is not mandatory (it may be optional).

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
 - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
 - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at <http://docbox.etsi.org/Reference>.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.