

ETSI EN 300 392-7 V3.3.1 (2012-07)



Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security

(<https://standards.iteh.ai>)
Document Preview

[ETSI EN 300 392-7 V3.3.1 \(2012-07\)](https://standards.iteh.ai/catalog/standards/etsi/f36bc189-9d32-4dcd-9d85-110eee9d453e/etsi-en-300-392-7-v3-3-1-2012-07)

<https://standards.iteh.ai/catalog/standards/etsi/f36bc189-9d32-4dcd-9d85-110eee9d453e/etsi-en-300-392-7-v3-3-1-2012-07>

Reference

REN/TETRA-06180

Keywords

security, TETRA, V+D

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

(<https://standards.iteh.ai>)
Document Preview

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 2012.
All rights reserved.

DECTTM, PLUGTESTSTM, UMTSTM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPPTM and LTETM are Trade Marks of ETSI registered for the benefit of its Members and
of the 3GPP Organizational Partners.
GSM[®] and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	10
Foreword.....	10
1 Scope	12
2 References	12
2.1 Normative references	12
2.2 Informative references.....	13
3 Definitions and abbreviations.....	13
3.1 Definitions	13
3.2 Abbreviations	16
4 Air Interface authentication and key management mechanisms	18
4.0 Security classes	18
4.1 Air interface authentication mechanisms	19
4.1.1 Overview	19
4.1.2 Authentication of an MS.....	19
4.1.3 Authentication of the infrastructure	20
4.1.4 Mutual authentication of MS and infrastructure	21
4.1.5 The authentication key.....	23
4.1.6 Equipment authentication	23
4.1.7 Authentication of an MS when migrated	24
4.1.8 Authentication of the home SwMI when migrated	25
4.1.9 Mutual Authentication of MS and infrastructure when migrated	26
4.2 Air Interface key management mechanisms.....	26
4.2.1 The DCK.....	26
4.2.2 The GCK.....	27
4.2.2.1 Session key modifier GCK0.....	28
4.2.3 The CCK.....	29
4.2.4 The SCK	30
4.2.4.1 SCK association for DMO use	31
4.2.4.1.1 DMO SCK subset grouping.....	32
4.2.5 The GSKO	34
4.2.5.1 SCK distribution to groups with OTAR.....	35
4.2.5.2 GCK distribution to groups with OTAR	35
4.2.5.3 Rules for MS response to group key distribution	36
4.2.6 Encrypted Short Identity (ESI) mechanism	36
4.2.7 Encryption Cipher Key	37
4.2.8 Summary of AI key management mechanisms.....	37
4.3 Service description and primitives	39
4.3.1 Authentication primitives	39
4.3.2 SCK transfer primitives	39
4.3.3 GCK transfer primitives.....	40
4.3.4 GSKO transfer primitives	41
4.4 Authentication protocol.....	42
4.4.1 Authentication state transitions.....	42
4.4.2 Authentication protocol sequences and operations	45
4.4.2.1 MSCs for authentication	46
4.4.2.2 MSCs for authentication Type-3 element	52
4.4.2.3 Control of authentication timer T354 at MS	55
4.5 OTAR protocols	56
4.5.1 CCK delivery - protocol functions.....	56
4.5.1.1 SwMI-initiated CCK provision	56
4.5.1.2 MS-initiated CCK provision with U-OTAR CCK demand.....	58
4.5.1.3 MS-initiated CCK provision with announced cell reselection	59
4.5.2 OTAR protocol functions - SCK	59
4.5.2.1 MS requests provision of SCK(s).....	60
4.5.2.2 SwMI provides SCK(s) to individual MS	61

4.5.2.3	SwMI provides SCK(s) to group of MSs	64
4.5.2.4	SwMI rejects provision of SCK	66
4.5.3	OTAR protocol functions - GCK	66
4.5.3.1	MS requests provision of GCK	66
4.5.3.2	SwMI provides GCK to an individual MS	69
4.5.3.3	SwMI provides GCK to a group of MSs	71
4.5.3.4	SwMI rejects provision of GCK	73
4.5.4	Cipher key association to group address	73
4.5.4.1	SCK association for DMO	74
4.5.4.2	GCK association	78
4.5.5	Notification of key change over the air	80
4.5.5.1	Change of DCK	82
4.5.5.2	Change of CCK	82
4.5.5.3	Change of GCK	82
4.5.5.4	Change of SCK for TMO	82
4.5.5.5	Change of SCK for DMO	83
4.5.5.6	Synchronization of Cipher Key Change	83
4.5.6	Security class change	83
4.5.6.1	Change of security class to security class 1	84
4.5.6.2	Change of security class to security class 2	84
4.5.6.3	Change of security class to security class 3	84
4.5.6.4	Change of security class to security class 3 with GCK	85
4.5.7	Notification of key in use	85
4.5.8	Notification of GCK Activation/Deactivation	85
4.5.9	Deletion of SCK, GCK and GSKO	85
4.5.10	Air Interface Key Status Enquiry	87
4.5.11	Crypto management group	90
4.5.12	OTAR retry mechanism	90
4.5.13	OTAR protocol functions - GSKO	91
4.5.13.1	MS requests provision of GSKO	91
4.5.13.2	SwMI provides GSKO to an MS	92
4.5.13.3	SwMI rejects provision of GSKO	93
4.5.14	OTAR protocol functions - interaction and queuing	93
4.5.15	KSOv for OTAR operations in visited SwMI	93
4.5.16	Transfer of AI cipher keys across the ISI	97

5	Enable and disable mechanism	97
5.1	General relationships	98
5.2	Enable/disable state transitions	98
5.3	Mechanisms	99
5.3.1	Disable of MS equipment	100
5.3.2	Disable of an subscription	100
5.3.3	Disable of subscription and equipment	100
5.3.4	Enable an MS equipment	100
5.3.5	Enable an MS subscription	100
5.3.6	Enable an MS equipment and subscription	100
5.4	Enable/disable protocol	101
5.4.1	General case	101
5.4.2	Status of cipher key material	102
5.4.2.1	Permanently disabled state	102
5.4.2.2	Temporarily disabled state	102
5.4.3	Specific protocol exchanges	103
5.4.3.1	Disabling an MS with mutual authentication	103
5.4.3.2	Enabling an MS with mutual authentication	105
5.4.3.3	Enabling an MS with non-mutual authentication	106
5.4.3.4	Disabling an MS with non-mutual authentication	107
5.4.4	Enabling an MS without authentication	108
5.4.5	Disabling an MS without authentication	109
5.4.6	Rejection of enable or disable command	109
5.4.6a	Expiry of Enable/Disable protocol timer	110
5.4.7	MM service primitives	111
5.4.7.1	TNMM-DISABLING primitive	111

5.4.7.2	TNMM-ENABLING primitive	111
6	Air Interface (AI) encryption	111
6.1	General principles.....	111
6.2	Security class.....	112
6.2.0	Notification of security class	113
6.2.0.1	Security Class of Neighbouring Cells	114
6.2.0.2	Identification of MS security capabilities	114
6.2.1	Constraints on LA arising from cell class	114
6.3	Key Stream Generator (KSG)	114
6.3.1	KSG numbering and selection	114
6.3.2	Interface parameters.....	115
6.3.2.1	Initial Value (IV).....	115
6.3.2.2	Cipher Key	115
6.4	Encryption mechanism	116
6.4.1	Allocation of KSS to logical channels.....	116
6.4.2	Allocation of KSS to logical channels with PDU association	118
6.4.2.1	General.....	118
6.4.2.2	KSS allocation on phase modulation channels.....	118
6.4.2.3	KSS allocation on QAM channels	120
6.4.2.3.1	Fixed mapping	120
6.4.2.3.2	Offset mapping	121
6.4.3	Synchronization of data calls where data is multi-slot interleaved	122
6.4.4	Recovery of stolen frames from interleaved data	123
6.5	Use of cipher keys	123
6.5.1	Identification of encryption state of downlink MAC PDUs	124
6.5.1.1	Class 1 cells.....	124
6.5.1.2	Class 2 cells.....	125
6.5.1.3	Class 3 cells.....	125
6.5.2	Identification of encryption state of uplink MAC PDUs	125
6.6	Mobility procedures	126
6.6.1	General requirements.....	126
6.6.1.1	Additional requirements for class 3 systems	126
6.6.2	Protocol description	126
6.6.2.1	Negotiation of ciphering parameters	126
6.6.2.1.1	Class 1 cells	126
6.6.2.1.2	Class 2 cells	127
6.6.2.1.3	Class 3 cells	127
6.6.2.2	Initial and undeclared cell re-selection.....	127
6.6.2.3	Unannounced cell re-selection	128
6.6.2.4	Announced cell re-selection type-3.....	129
6.6.2.5	Announced cell re-selection type-2.....	129
6.6.2.6	Announced cell re-selection type-1.....	129
6.6.2.7	Key forwarding	129
6.6.3	Shared channels	131
6.7	Encryption control.....	131
6.7.1	Data to be encrypted	131
6.7.1.1	Downlink control channel requirements	131
6.7.1.2	Encryption of MAC header elements.....	131
6.7.1.3	Traffic channel encryption control.....	131
6.7.1.4	Handling of PDUs that do not conform to negotiated ciphering mode	132
6.7.2	Service description and primitives.....	132
6.7.2.1	Mobility Management (MM)	133
6.7.2.2	Mobile Link Entity (MLE).....	134
6.7.2.3	Layer 2	136
6.7.3	Protocol functions	136
6.7.3.1	MM	136
6.7.3.2	MLE	136
6.7.3.3	LLC	136
6.7.3.4	MAC	137
6.7.4	PDUs for cipher negotiation	137

Annex A (normative):	PDU and element definitions	138
A.1	Authentication PDUs	138
A.1.1	D-AUTHENTICATION demand	138
A.1.2	D-AUTHENTICATION reject	138
A.1.3	D-AUTHENTICATION response	139
A.1.4	D-AUTHENTICATION result	139
A.1.5	U-AUTHENTICATION demand	139
A.1.6	U-AUTHENTICATION reject	140
A.1.7	U-AUTHENTICATION response	140
A.1.8	U-AUTHENTICATION result	141
A.2	OTAR PDUs	141
A.2.1	D-OTAR CCK Provide	141
A.2.2	U-OTAR CCK Demand	141
A.2.3	U-OTAR CCK Result	142
A.2.4	D-OTAR GCK Provide	142
A.2.5	U-OTAR GCK Demand	143
A.2.6	U-OTAR GCK Result	144
A.2.6a	D-OTAR GCK Reject	144
A.2.7	D-OTAR SCK Provide	145
A.2.8	U-OTAR SCK Demand	146
A.2.9	U-OTAR SCK Result	146
A.2.9a	D-OTAR SCK Reject	147
A.2.10	D-OTAR GSKO Provide	147
A.2.11	U-OTAR GSKO Demand	148
A.2.12	U-OTAR GSKO Result	148
A.2.12a	D-OTAR GSKO Reject	148
A.3	PDUs for key association to GTSI	149
A.3.1	D-OTAR KEY ASSOCIATE demand	149
A.3.2	U-OTAR KEY ASSOCIATE status	150
A.4	PDUs to synchronize key or security class change	150
A.4.1	D-CK CHANGE demand	150
A.4.2	U-CK CHANGE result	151
A.4.2a	U-OTAR KEY DELETE result	152
A.4.2b	U-OTAR KEY STATUS response	153
A.4.3	D-DM-SCK ACTIVATE DEMAND	154
A.4.4	U-DM-SCK ACTIVATE RESULT	155
A.4a	PDUs to delete air interface keys in MS	156
A.4a.1	D-OTAR KEY DELETE demand	156
A.4a.2	U-OTAR KEY DELETE result	156
A.4b	PDUs to obtain Air Interface Key Status	157
A.4b.1	D-OTAR KEY STATUS demand	157
A.4b.2	U-OTAR KEY STATUS response	158
A.5	Other security domain PDUs	159
A.5.1	U-TEI PROVIDE	159
A.5.2	U-OTAR PREPARE	160
A.5.3	D-OTAR NEWCELL	160
A.5.4	D-OTAR CMG GTSI PROVIDE	160
A.5.5	U-OTAR CMG GTSI RESULT	161
A.6	PDUs for Enable and Disable	161
A.6.1	D-DISABLE	161
A.6.2	D-ENABLE	162
A.6.3	U-DISABLE STATUS	162
A.7	MM PDU type 3 information elements coding	163
A.7.1	Authentication downlink	163
A.7.2	Authentication uplink	163

A.8	PDU Information elements coding.....	164
A.8.1	Acknowledgement flag.....	164
A.8.2	Address extension.....	164
A.8.3	Authentication challenge.....	164
A.8.4	Authentication reject reason.....	164
A.8.5	Authentication result	165
A.8.6	Authentication sub-type	165
A.8.7	CCK identifier	165
A.8.8	CCK information.....	165
A.8.9	CCK Location area information	166
A.8.10	CCK request flag.....	166
A.8.11	Change of security class	166
A.8.12	Ciphering parameters	167
A.8.13	CK provision flag	167
A.8.14	CK provisioning information	167
A.8.15	CK request flag.....	168
A.8.16	Class Change flag.....	168
A.8.17	DCK forwarding result.....	168
A.8.18	Disabling type	168
A.8.19	Enable/Disable result.....	169
A.8.20	Encryption mode	169
A.8.20.1	Class 1 cells	169
A.8.20.2	Class 2 cells	169
A.8.20.3	Class 3 cells	170
A.8.21	Equipment disable	170
A.8.22	Equipment enable	170
A.8.23	Equipment status	170
A.8.23a	Explicit response	171
A.8.24	Frame number	171
A.8.25	Future key flag	171
A.8.26	GCK data.....	171
A.8.27	GCK key and identifier	171
A.8.28	GCK Number (GCKN)	172
A.8.28a	GCK Provision result	172
A.8.28b	GCK rejected.....	172
A.8.29	GCK select number	172
A.8.29a	GCK Supported.....	173
A.8.30	GCK Version Number (GCK-VN).....	173
A.8.31	Group association	173
A.8.31a	Group Identity Security Related Information.....	174
A.8.32	GSKO Version Number (GSKO-VN).....	174
A.8.33	GSSI	174
A.8.34	Hyperframe number	174
A.8.35	Intent/confirm.....	174
A.8.36	Void.....	175
A.8.37	Key association status	175
A.8.38	Key association type.....	175
A.8.39	Key change type	175
A.8.39a	Key delete type.....	176
A.8.39b	Key status type	176
A.8.39c	Key delete extension	176
A.8.40	Key type flag	177
A.8.41	KSG-number	177
A.8.42	Location area	177
A.8.43	Location area bit mask	177
A.8.44	Location area selector.....	177
A.8.45	Location area list	178
A.8.46	Location area range	178
A.8.46a	Max response timer value.....	178
A.8.47	Mobile country code.....	178
A.8.48	Mobile network code.....	178
A.8.49	Multiframe number.....	178