

ETSI TS 100 392-7 V4.1.1 (2022-10)



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

[ETSI TS 100 392-7 V4.1.1 \(2022-10\)](https://standards.iteh.ai/catalog/standards/sist/5538fd58-549b-409e-b4a5-46e8267c91ff/etsi-ts-100-392-7-v4-1-1-2022-10)

<https://standards.iteh.ai/catalog/standards/sist/5538fd58-549b-409e-b4a5-46e8267c91ff/etsi-ts-100-392-7-v4-1-1-2022-10>

ReferenceRTS/TCCE-06208

Keywordssecurity, 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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:

<http://www.etsi.org/standards-search>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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

<https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx>

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

<https://standards-portal.etsi.org/People/CommitteeSupportStaff.aspx>

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:

<https://www.etsi.org/standards/coordinated-vulnerability-disclosure>

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2022.
All rights reserved.

Contents

Intellectual Property Rights	12
Foreword.....	12
Modal verbs terminology.....	13
1 Scope	14
2 References	14
2.1 Normative references	14
2.2 Informative references.....	15
3 Definition of terms, symbols and abbreviations.....	16
3.1 Terms.....	16
3.2 Symbols.....	20
3.3 Abbreviations	20
4 Air Interface authentication and key management mechanisms	23
4.a General	23
4.0 Security classes	23
4.1 Air interface authentication mechanisms	24
4.1.1 Overview	24
4.1.1a Authentication and key management algorithms.....	25
4.1.2 Authentication of an MS.....	25
4.1.3 Authentication of the infrastructure	28
4.1.4 Mutual authentication of MS and infrastructure	30
4.1.5 The authentication key.....	35
4.1.6 Equipment authentication	35
4.1.6a Request for information related to an MS.....	36
4.1.7 Authentication of an MS when migrated	36
4.1.8 Authentication of the home SwMI when migrated.....	39
4.1.9 Mutual Authentication of MS and infrastructure when migrated	41
4.2 Air Interface key management mechanisms.....	41
4.2.0 General.....	41
4.2.1 The Derived Cipher Key.....	42
4.2.1.1 DCK and DCKX overview	42
4.2.1.2 DCK derivation	42
4.2.1.3 DCKX derivation	42
4.2.1.4 Usage of DCK and DCKX.....	43
4.2.1.5 Validity of DCK and DCKX.....	43
4.2.2 The Group Cipher Key	43
4.2.2.0 General.....	43
4.2.2.0a Validity of GCK and GCKX.....	44
4.2.2.0b Distribution of GCK.....	44
4.2.2.0c Distribution of GCKX.....	44
4.2.2.0d Decryption of sealed GCK and GCKX.....	45
4.2.2.0e Summary of GCK distribution process	45
4.2.2.1 Session key modifiers GCK0 and GCKX0	47
4.2.3 The Common Cipher Key.....	47
4.2.3.1 CCK and CCKX usage.....	47
4.2.3.2 CCK and CCKX identification	48
4.2.3.3 CCK and CCKX distribution	48
4.2.3.4 CCK and CCKX validity	49
4.2.4 The Static Cipher Key.....	49
4.2.4.0 General.....	49
4.2.4.0a SCK sets.....	50
4.2.4.0b SCK and SCKX identification	50
4.2.4.0c Distribution of SCK	50
4.2.4.0d Distribution of SCKX	51
4.2.4.0e Decryption of sealed SCK and SCKX	51

4.2.4.0f	Summary of SCK distribution process	51
4.2.4.1	SCK association for DMO use	54
4.2.4.1.0	General	54
4.2.4.1.1	DMO SCK subset grouping.....	54
4.2.5	The Group Session Key for OTAR.....	57
4.2.5.0	General	57
4.2.5.0a	Validity of GSKO and GSKOX	57
4.2.5.0b	Distribution of GSKO and GSKOX.....	58
4.2.5.1	SCK and SCKX distribution to groups with OTAR	59
4.2.5.2	GCK and GCKX distribution to groups with OTAR	60
4.2.5.3	Rules for MS response to group key distribution	60
4.2.5a	OTAR of migrated MS	60
4.2.5a.1	Visited Session Keys for OTAR	60
4.2.5a.2	Derivation of KSOv	60
4.2.5a.3	Derivation of KSOXv	61
4.2.5a.4	OTAR of CKX to migrated MS where home SwMI supports an air interface encryption algorithm from TEA set A	62
4.2.5a.5	OTAR of CK to migrated MS where home SwMI supports an air interface encryption algorithm from TEA set B	63
4.2.6	Encrypted Short Identity (ESI) mechanism	63
4.2.7	Encryption Cipher Key	65
4.2.8	Summary of AI key management mechanisms.....	66
4.3	Service description and primitives	68
4.3.1	Authentication primitives	68
4.3.2	Static Cipher Key transfer primitives.....	69
4.3.3	Group Cipher Key transfer primitives	70
4.3.4	Group Session Key for OTAR transfer primitives.....	71
4.4	Authentication protocol.....	71
4.4.1	Authentication state transitions.....	71
4.4.2	Authentication protocol sequences and operations	74
4.4.2.0	General	74
4.4.2.1	MSCs for authentication	76
4.4.2.2	MSCs for authentication and security type-3 elements	82
4.4.2.3	Control of authentication timer T354 at MS	86
4.4a	Information request protocol	87
4.5	OTAR protocols	90
4.5.1	Common Cipher Key delivery - protocol functions.....	90
4.5.1.0	General	90
4.5.1.1	SwMI-initiated CCK and CCKX provision	91
4.5.1.2	MS-initiated CCK provision with U-OTAR CCK DEMAND.....	93
4.5.1.3	MS-initiated CCK or CCKX provision with announced cell reselection.....	93
4.5.2	OTAR protocol functions - Static Cipher Key.....	94
4.5.2.0	General	94
4.5.2.1	MS requests provision of SCK(s) or SCKX(s).....	95
4.5.2.2	SwMI provides SCK(s) or SCKX(s) to individual MS	97
4.5.2.3	SwMI provides SCK(s) or SCKX(s) to group of MSs	98
4.5.2.4	SwMI rejects provision of SCK or SCKX	99
4.5.3	OTAR protocol functions - Group Cipher Key.....	100
4.5.3.0	General	100
4.5.3.1	MS requests provision of GCK or GCKX.....	100
4.5.3.2	SwMI provides GCK or GCKX to an individual MS	103
4.5.3.3	SwMI provides GCK or GCKX to a group of MSs	104
4.5.3.4	SwMI rejects provision of GCK or GCKX	105
4.5.4	Cipher key association to group address.....	106
4.5.4.0	General	106
4.5.4.1	Static Cipher Key association for DMO.....	106
4.5.4.2	Group Cipher Key association	109
4.5.5	Notification of key change over the air.....	111
4.5.5.0	General	111
4.5.5.1	Change of Derived Cipher Key.....	112
4.5.5.2	Change of Common Cipher Key	113
4.5.5.3	Change of Group Cipher Key.....	113

4.5.5.4	Change of Static Cipher Key for TMO	113
4.5.5.5	Change of Static Cipher Key for DMO.....	113
4.5.5.6	Synchronization of Cipher Key Change	114
4.5.6	Security class change	114
4.5.6.0	General	114
4.5.6.1	Change of security class to security class 1	115
4.5.6.2	Change of security class to security class 2	115
4.5.6.3	Change of security class to security class 3	115
4.5.6.4	Change of security class to security class 3 with GCK or GCKX.....	116
4.5.7	Notification of key in use.....	116
4.5.8	Notification of GCK or GCKX Activation/Deactivation.....	116
4.5.9	Deletion of SCK/SCKX, GCK/GCKX and GSKO/GSKOX	116
4.5.10	Air Interface Key Status Enquiry.....	119
4.5.11	Crypto management group.....	121
4.5.12	OTAR retry mechanism.....	122
4.5.13	OTAR protocol functions - Group Session Key for OTAR.....	122
4.5.13.0	General	122
4.5.13.1	MS requests provision of GSKO or GSKOX.....	123
4.5.13.2	SwMI provides GSKO or GSKOX to an MS.....	123
4.5.13.3	SwMI rejects provision of GSKO or GSKOX	124
4.5.14	OTAR protocol functions - interaction and queuing.....	124
4.5.15	Session Key for OTAR operations in visited SwMI.....	124
4.5.15.1	General	124
4.5.15.2	Home and visited SwMI use air interface encryption algorithms from the same algorithm set.....	125
4.5.15.3	Home and visited SwMI use air interface encryption algorithms from different algorithm sets.....	128
4.5.16	Transfer of AI cipher keys across the ISI	130
5	Enable and disable mechanism.....	130
5.0	General	130
5.1	General relationships	130
5.2	Enable/disable state transitions.....	131
5.3	Mechanisms.....	132
5.3.0	General.....	132
5.3.1	Disable of MS equipment	133
5.3.2	Disable of an subscription.....	133
5.3.3	Disable of subscription and equipment	133
5.3.4	Enable an MS equipment	133
5.3.5	Enable an MS subscription	133
5.3.6	Enable an MS equipment and subscription.....	133
5.4	Enable/disable protocol	134
5.4.1	General case.....	134
5.4.2	Status of cipher key material.....	135
5.4.2.1	Permanently disabled state	135
5.4.2.2	Temporarily disabled state	135
5.4.3	Specific protocol exchanges	136
5.4.3.0	General	136
5.4.3.1	Disabling an MS with mutual authentication	136
5.4.3.2	Enabling an MS with mutual authentication	137
5.4.3.3	Enabling an MS with non-mutual authentication.....	138
5.4.3.4	Disabling an MS with non-mutual authentication.....	140
5.4.4	Enabling an MS without authentication.....	141
5.4.5	Disabling an MS without authentication.....	141
5.4.6	Rejection of enable or disable command	141
5.4.6a	Expiry of Enable/Disable protocol timer	142
5.4.7	MM service primitives.....	142
5.4.7.0	General	142
5.4.7.1	TNMM-DISABLING primitive.....	143
5.4.7.2	TNMM-ENABLING primitive.....	143
6	Air Interface (AI) encryption	143
6.1	General principles.....	143
6.2	Security class.....	144

6.2.a	General.....	144
6.2.0	Notification of security class	145
6.2.0.0	General.....	145
6.2.0.1	Security class of neighbouring Cells.....	146
6.2.0.2	Identification of MS security capabilities	146
6.2.1	Constraints on LA arising from cell class.....	146
6.3	Key Stream Generator (KSG)	147
6.3.0	General.....	147
6.3.1	KSG numbering and selection	147
6.3.2	Interface parameters.....	148
6.3.2.0	General	148
6.3.2.0a	IV validity	148
6.3.2.1	Initial Value (IV) for algorithms in TEA set A	149
6.3.2.2	Cipher Key for algorithms in TEA set A	149
6.3.2.3	Initial Value (IV) for algorithms in TEA set B	150
6.3.2.4	Cipher Key for algorithms in TEA set B.....	151
6.4	Encryption mechanism	151
6.4.0	General.....	151
6.4.1	Allocation of KSS to logical channels.....	152
6.4.2	Allocation of KSS to logical channels.....	153
6.4.2.1	General	153
6.4.2.2	KSS allocation on phase modulation channels.....	154
6.4.2.3	KSS allocation on QAM channels for algorithms in TEA set A.....	158
6.4.2.3.0	General	158
6.4.2.3.1	Fixed mapping	159
6.4.2.3.2	Offset mapping.....	160
6.4.2.4	KSS allocation on QAM channels for algorithms in TEA set B.....	161
6.4.3	Synchronization of data calls where data is multi-slot interleaved	163
6.4.4	Recovery of stolen frames from interleaved data	163
6.5	Use of cipher keys	164
6.5.0	General.....	164
6.5.1	Identification of encryption state of downlink MAC PDUs	165
6.5.1.0	General	165
6.5.1.1	Class 1 cells.....	165
6.5.1.2	Class 2 cells.....	166
6.5.1.3	Class 3 cells.....	166
6.5.2	Identification of encryption state of uplink MAC PDUs	166
6.6	Mobility procedures	167
6.6.1	General requirements.....	167
6.6.1.0	Common requirements	167
6.6.1.1	Additional requirements for class 3 systems	167
6.6.2	Protocol description	167
6.6.2.0	General	167
6.6.2.1	Negotiation of ciphering parameters	167
6.6.2.1.0	General	167
6.6.2.1.1	Class 1 cells.....	168
6.6.2.1.2	Class 2 cells.....	168
6.6.2.1.3	Class 3 cells.....	168
6.6.2.2	Initial and undeclared cell re-selection.....	168
6.6.2.3	Unannounced cell re-selection	170
6.6.2.4	Announced cell re-selection type-3.....	171
6.6.2.5	Announced cell re-selection type-2.....	171
6.6.2.6	Announced cell re-selection type-1.....	171
6.6.2.7	Key forwarding	171
6.6.3	Shared channels	172
6.7	Encryption control.....	173
6.7.0	General.....	173
6.7.1	Data to be encrypted	173
6.7.1.1	Downlink control channel requirements	173
6.7.1.2	Encryption of MAC header elements.....	173
6.7.1.2a	MAC Address Encryption mechanism for KSGs in TEA set B.....	174
6.7.1.2a.1	Usage of MAC Address Encryption mechanism.....	174

6.7.1.2a.2	MAE operation	174
6.7.1.2a.3	Addresses to be encrypted	175
6.7.1.3	Traffic channel encryption control	176
6.7.1.4	Handling of PDUs that do not conform to negotiated ciphering mode	176
6.7.2	Service description and primitives	176
6.7.2.0	General	176
6.7.2.1	Mobility Management (MM)	177
6.7.2.2	Mobile Link Entity (MLE)	178
6.7.2.3	Layer 2	180
6.7.3	Protocol functions	180
6.7.3.0	General	180
6.7.3.1	MM	180
6.7.3.2	MLE	180
6.7.3.3	LLC	180
6.7.3.4	MAC	181
6.7.4	PDUs for cipher negotiation	181
Annex A (normative):	PDU and element definitions	182
A.0	General	182
A.1	Authentication PDUs	182
A.1.1	D-AUTHENTICATION DEMAND	182
A.1.2	D-AUTHENTICATION REJECT	182
A.1.3	D-AUTHENTICATION RESPONSE	183
A.1.4	D-AUTHENTICATION RESULT	183
A.1.5	U-AUTHENTICATION DEMAND	183
A.1.6	U-AUTHENTICATION REJECT	184
A.1.7	U-AUTHENTICATION RESPONSE	184
A.1.8	U-AUTHENTICATION RESULT	185
A.2	OTAR PDUs	185
A.2.1	D-OTAR CCK PROVIDE	185
A.2.1a	D-OTAR CCKX PROVIDE	185
A.2.2	U-OTAR CCK DEMAND	186
A.2.3	U-OTAR CCK RESULT	186
A.2.4	D-OTAR GCK PROVIDE	187
A.2.4a	D-OTAR GCKX PROVIDE	188
A.2.5	U-OTAR GCK DEMAND	188
A.2.6	U-OTAR GCK RESULT	189
A.2.6a	D-OTAR GCK REJECT	189
A.2.7	D-OTAR SCK PROVIDE	190
A.2.7a	D-OTAR SCKX PROVIDE	191
A.2.8	U-OTAR SCK DEMAND	191
A.2.9	U-OTAR SCK RESULT	192
A.2.9a	D-OTAR SCK REJECT	192
A.2.10	D-OTAR GSKO PROVIDE	193
A.2.10a	D-OTAR GSKOX PROVIDE	193
A.2.11	U-OTAR GSKO DEMAND	194
A.2.12	U-OTAR GSKO RESULT	194
A.2.12a	D-OTAR GSKO REJECT	195
A.3	PDUs for key association to GTSI	195
A.3.1	D-OTAR KEY ASSOCIATE DEMAND	195
A.3.2	U-OTAR KEY ASSOCIATE STATUS	196
A.4	PDUs to synchronize key or security class change	197
A.4.1	D-CK CHANGE DEMAND	197
A.4.2	U-CK CHANGE RESULT	198
A.4.2a	Void	198
A.4.2b	Void	198
A.4.3	D-DM-SCK ACTIVATE DEMAND	198
A.4.4	U-DM-SCK ACTIVATE RESULT	199

A.4a	PDUs to delete air interface keys in MS	200
A.4a.1	D-OTAR KEY DELETE DEMAND	200
A.4a.2	U-OTAR KEY DELETE RESULT	200
A.4b	PDUs to obtain Air Interface Key Status	201
A.4b.1	D-OTAR KEY STATUS DEMAND	201
A.4b.2	U-OTAR KEY STATUS RESPONSE	202
A.5	Other security domain PDUs	203
A.5.1	U-TEI PROVIDE	203
A.5.2	U-OTAR PREPARE	204
A.5.3	D-OTAR NEWCELL	204
A.5.3a	D-OTAR NEWCELL-X	204
A.5.4	D-OTAR CMG GTSI PROVIDE	205
A.5.5	U-OTAR CMG GTSI RESULT	206
A.5.6	U-INFORMATION PROVIDE	206
A.6	PDUs for Enable and Disable	208
A.6.1	D-DISABLE	208
A.6.2	D-ENABLE	208
A.6.3	U-DISABLE STATUS	209
A.7	MM PDU type 3 information elements coding	209
A.7.0	General	209
A.7.1	Authentication downlink	209
A.7.2	Authentication uplink	210
A.7.3	Security downlink	210
A.8	PDU Information elements coding	212
A.8.0	General	212
A.8.1	Acknowledgement flag	212
A.8.1a	Additional information present	212
A.8.1b	Additional security	212
A.8.2	Address extension	212
A.8.2a	AI algorithm information present	213
A.8.2b	AI algorithm information request flag	213
A.8.3	Authentication challenge	213
A.8.4	Authentication reject reason	213
A.8.5	Authentication result	213
A.8.6	Authentication sub-type	214
A.8.7	CCK identifier	214
A.8.8	CCK information	214
A.8.9	CCK Location area information	215
A.8.10	CCK request flag	215
A.8.11	Change of security class	215
A.8.12	Ciphering parameters	216
A.8.13	CK provision flag	216
A.8.14	CK provision information	216
A.8.15	CK request flag	217
A.8.16	Class Change flag	217
A.8.17	DCK forwarding result	217
A.8.18	Disabling type	217
A.8.19	Enable/Disable result	218
A.8.20	Encryption mode	218
A.8.20.1	Class 1 cells	218
A.8.20.2	Class 2 cells	218
A.8.20.3	Class 3 cells	218
A.8.21	Equipment disable	219
A.8.22	Equipment enable	219
A.8.23	Equipment status	219
A.8.23a	Explicit response	219
A.8.24	Frame number	219
A.8.24a	Future information present	220

A.8.25	Future key flag	220
A.8.26	GCK data.....	220
A.8.27	GCK key and identifier	220
A.8.27a	GCKX key and identifier	220
A.8.28	GCK Number (GCKN)	221
A.8.28a	GCK Provision result	221
A.8.28b	GCK rejected.....	221
A.8.29	GCK select number	221
A.8.29a	GCK Supported.....	222
A.8.30	GCK Version Number (GCK-VN).....	222
A.8.31	Group association	222
A.8.31a	Group Identity Security Related Information.....	223
A.8.32	GSKO Version Number (GSKO-VN).....	223
A.8.33	GSSI.....	223
A.8.33a	HW SW version request flag.....	223
A.8.33b	HW version number present.....	224
A.8.34	Hyperframe number	224
A.8.34a	Identity encryption	224
A.8.35	Intent/confirm.....	224
A.8.36	Void.....	224
A.8.37	Key association status	225
A.8.38	Key association type.....	225
A.8.39	Key change type	225
A.8.39a	Key delete type.....	225
A.8.39b	Key status type	226
A.8.39c	Key delete extension	226
A.8.40	Key type flag	226
A.8.41	KSG-number	227
A.8.42	Location area	227
A.8.43	Location area bit mask	227
A.8.44	Location area selector.....	227
A.8.45	Location area list	228
A.8.46	Location area range	228
A.8.46a	Max response timer value.....	228
A.8.47	Mobile country code.....	228
A.8.48	Mobile network code.....	228
A.8.48a	Model number information present	229
A.8.48b	Model number request flag.....	229
A.8.49	Multiframe number.....	229
A.8.50	Mutual authentication flag.....	229
A.8.51	Network time	229
A.8.52	Number of GCKs changed	229
A.8.52a	Number of GCKs deleted	230
A.8.52b	Number of GCK status	230
A.8.52c	Number of GCKs provided	230
A.8.52d	Number of GCKs rejected.....	231
A.8.52e	Number of GCKs requested by GCKN	231
A.8.52f	Number of GCKs requested by GSSI.....	231
A.8.53	Number of groups.....	232
A.8.53a	Number of GSKO status.....	232
A.8.53b	Number of KSGs present	232
A.8.54	Number of location areas	232
A.8.55	Number of SCKs changed.....	233
A.8.55a	Number of SCKs deleted.....	233
A.8.56	Number of SCKs provided	233
A.8.56a	Number of SCKs rejected.....	233
A.8.57	Number of SCKs requested	234
A.8.57a	Number of SCK status.....	234
A.8.57b	OTAR reject reason.....	235
A.8.57c	OTAR retry interval	235
A.8.58	OTAR sub-type	235
A.8.58a	OTAR extension.....	236

A.8.59	PDU type	236
A.8.60	Proprietary	237
A.8.61	Provision result	237
A.8.62	Random challenge	237
A.8.63	Random seed	237
A.8.64	Random seed for OTAR	238
A.8.65	Void	238
A.8.65a	Reject reason	238
A.8.66	Response value	238
A.8.67	SCK data	238
A.8.68	SCK information	239
A.8.69	SCK key and identifier	239
A.8.69a	SCKX key and identifier	239
A.8.70	SCK Number (SCKN)	239
A.8.71	SCK number and result	240
A.8.72	SCK provision flag	240
A.8.72a	Void	240
A.8.72b	SCK rejected	240
A.8.73	SCK select number	241
A.8.73a	SCK subset grouping type	241
A.8.73b	SCK subset number	242
A.8.74	SCK use	242
A.8.75	SCK version number	242
A.8.76	Sealed CCK, Sealed SCK, Sealed GCK, Sealed GSKO	242
A.8.76a	Sealed CCKX, Sealed SCKX, Sealed GCKX	243
A.8.76b	Sealed GSKOX	243
A.8.77	Security information element	243
A.8.77a	Security parameters	245
A.8.77b	Security related information element	245
A.8.78	Session key	245
A.8.79	Slot Number	246
A.8.80	SSI	246
A.8.81	Subscription disable	246
A.8.82	Subscription enable	246
A.8.83	Subscription status	246
A.8.83a	SW version number present	247
A.8.84	TEI	247
A.8.85	TEI request flag	247
A.8.86	Time type	248
A.8.87	Type 3 element identifier	248

Annex B (normative): Boundary conditions for the cryptographic algorithms and procedures249

B.0	General	249
B.1	Dimensioning of the cryptographic parameters	258
B.2	Summary of the cryptographic processes	260

Annex C (normative): Timers274

C.1	T354, authentication protocol timer	274
C.2	T371, delay timer for group addressed delivery of SCK/SCKX and GCK/GCKX	274
C.3	T372, key forwarding timer	274
C.4	T355, disable control timer	274

Annex D (informative): Transition between air interface encryption algorithms in TEA set A and TEA set B275

D.1	Overview	275
-----	----------------	-----

D.2	Algorithm support	275
D.2.1	General	275
D.2.2	SwMI dependencies	276
D.2.3	MSs able to support more than one algorithm.....	276
D.2.4	MSs only able to support one algorithm.....	276
D.3	Group and broadcast communication during transition	277
D.3.1	Group communication.....	277
D.3.2	Broadcast communications.....	277
D.4	Transition scenarios for TMO	277
D.4.1	Transition overview.....	277
D.4.2	Encryption class while loading set B algorithm to MSs.....	278
D.4.3	Encryption during transition.....	279
D.5	Transition scenarios for DMO.....	280
D.5.1	General	280
D.5.2	MS to MS DMO operation.....	280
D.5.3	DMO repeater operation.....	280
D.5.4	DMO gateway operation	281
Annex E (informative):	Bibliography.....	282
Annex F (informative):	Change request history.....	283
History		284

i T h S T A N D A R D P R E
(s t a n d a r d s . i t e h)

E T S I T S 1 0 0 3 9 2 - 7
h t t p s : / / s t a n d a r d s . i t e h . a
4 6 e 8 f 2 / 6 e 7 t c s 9 f f s - 1 0 0 - 3 9

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 (<https://ipr.etsi.org/>).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee TETRA and Critical Communications Evolution (TCCE).

The present document is part 7 of a multi-part deliverable covering the Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D), Release 2, as identified below:

- Part 1: "General network design";
- Part 2: "Air Interface (AI)";
- Part 3: "Interworking at the Inter-System Interface (ISI)";
- Part 4: "Gateways basic operation";
- Part 5: "Peripheral Equipment Interface (PEI)";
- Part 7: "Security";**
- Part 9: "General requirements for supplementary services";
- Part 10: "Supplementary services stage 1";
- Part 11: "Supplementary services stage 2";
- Part 12: "Supplementary services stage 3";
- Part 13: "SDL model of the Air Interface (AI)";
- Part 14: "Protocol Implementation Conformance Statement (PICS) proforma specification";
- Part 15: "TETRA frequency bands, duplex spacings and channel numbering";
- Part 16: "Network Performance Metrics";

Part 17: "TETRA V+D and DMO specifications";

Part 18: "Air interface optimized applications";

Part 19: "Interworking between TETRA and Broadband systems".

NOTE 1: Part 3, sub-parts 6 and 7 (Speech format implementation), part 4, sub-part 3 (Data networks gateway), part 10, sub-part 15 (Transfer of control), part 13 (SDL) and part 14 (PICS) of this multi-part deliverable are in status "historical" and are not maintained.

NOTE 2: Some parts are also published as Technical Specifications such as ETSI TS 100 392-7 (the present document) and those may be the latest version of the document.

Modal verbs terminology

In the present document "shall", "shall not", "should", "should not", "may", "need not", "will", "will not", "can" and "cannot" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"must" and "must not" are **NOT** allowed in ETSI deliverables except when used in direct citation.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ETSI TS 100 392-7 V4.1.1 (2022-10)

<https://standards.iteh.ai/catalog/standards/sist/5538fd58-549b-409e-b4a5-46e8267c91ff/etsi-ts-100-392-7-v4-1-1-2022-10>

1 Scope

The present document defines the Terrestrial Trunked Radio system (TETRA) supporting Voice plus Data (V+D). It specifies the air interface, the inter-working between TETRA systems and to other systems via gateways, the terminal equipment interface on the mobile station, the connection of line stations to the infrastructure, the security aspects in TETRA networks, the management services offered to the operator, the performance objectives, and the supplementary services that come in addition to the basic and teleservices.

The present part describes the security mechanisms in TETRA V+D. It provides mechanisms for confidentiality of control signalling and user speech and data at the air interface, authentication and key management mechanisms for the air interface and for the Inter-System Interface (ISI).

Clause 4 describes the authentication and key management mechanisms for the TETRA air interface. The following authentication services have been specified for the air-interface in ETSI ETR 086-3 [i.3], based on a threat analysis:

- authentication of an MS by the TETRA infrastructure;
- authentication of the TETRA infrastructure by an MS;
- mutual authentication of MS and TETRA infrastructure.

The key management mechanisms specified in clause 4 enable the provision of key material for the air interface encryption mechanisms specified in clause 6.

Clause 5 describes the mechanisms and protocol for enable and disable of both the mobile station equipment and the mobile station user's subscription.

Air interface encryption may be provided as an option in TETRA. Where employed, clause 6 describes the confidentiality mechanisms using encryption on the air interface, for circuit mode speech, circuit mode data, packet data and control information. Clause 6 describes both encryption mechanisms and mobility procedures. It also details the protocol concerning control of encryption at the air interface. Encryption mechanisms and control protocol are specified for two different air interface encryption algorithm sets.

Annex A specifies the Protocol Data Units and Information Elements required to fulfil the protocols specified in clauses 4, 5 and 6. Annex B specifies boundary conditions, dimensioning and summaries of the cryptographic algorithms, parameters and processes specified in the present document. Annex C specifies timer values used within the protocols. Annex D provides considerations for a transition process between the usage of encryption algorithms from different air interface encryption algorithm sets.

The present document does not address the detail handling of protocol errors or any protocol mechanisms when TETRA is operating in a degraded mode. These issues are implementation specific and therefore fall outside the scope of the TETRA standardization effort.

The detail description of the Authentication Centre is outside the scope of the present document.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE 1: Some referenced ENs are also published as Technical Specifications. In all cases, the latest version of such a document, either EN or TS, should be taken as the referenced document.

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

NOTE 2: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

- [1] ETSI EN 300 392-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".
- [2] ETSI EN 300 392-2: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".
- [3] ISO 7498-2: "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".
- [4] ETSI EN 300 812-3: "Terrestrial Trunked Radio (TETRA); Subscriber Identity Module to Mobile Equipment (SIM-ME) interface; Part 3: Integrated Circuit (IC); Physical, logical and TSIM application characteristics".
- [5] ETSI EN 300 396-6: "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".
- [6] ETSI EN 302 109: "Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption".
- [7] ETSI EN 300 392-12-22: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 12: Supplementary services stage 3; Sub-part 22: Dynamic Group Number Assignment (DGNA)".
- [8] ETSI EN 300 392-3-5: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 5: Additional Network Feature for Mobility Management (ANF-ISIMM)".
- [9] ETSI EN 300 396-1: "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 1: General network design".
- [10] ETSI ES 200 812-2: "Terrestrial Trunked Radio (TETRA); Subscriber Identity Module to Mobile Equipment (TSIM-ME) interface; Part 2: Universal Integrated Circuit Card (UICC); Characteristics of the TSIM application".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [i.1] ETSI ETS 300 392-2 (1996): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".
- [i.2] ETSI ETS 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".
- [i.3] ETSI ETR 086-3: "Trans European Trunked Radio (TETRA) systems; Technical requirements specification; Part 3: Security aspects".
- [i.4] ETSI EN 300 392-7 (V2.2.1): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".
- [i.5] ETSI EN 300 392-7 (V2.1.1): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".
- [i.6] ETSI TS 100 392-18-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D) and Direct Mode Operation (DMO); Part 18: Air interface optimized applications; Sub-part 1: Location Information Protocol (LIP)".