

ETSI EN 300 392-7 V3.4.1 (2017-01)



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

Full standard (standards.iteh.ai/catalog/standards/sis/300-392-7-v3.4.1-2017-01)
<https://standards.iteh.ai/catalog/standards/sis/300-392-7-v3.4.1-2017-01>
4685-a9bc-3bb5c4641eb8/etsi-en-300-392-7-v3.4.1-2017-01

Reference

REN/TETRA-06184

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

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 only prevailing document is the print of the Portable Document Format (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

<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://portal.etsi.org/People/CommiteeSupportStaff.aspx>

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.

© European Telecommunications Standards Institute 2017.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** 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	11
Foreword.....	11
Modal verbs terminology.....	12
1 Scope	13
2 References	13
2.1 Normative references	13
2.2 Informative references.....	14
3 Definitions and abbreviations.....	15
3.1 Definitions.....	15
3.2 Abbreviations	18
4 Air Interface authentication and key management mechanisms	20
4.a General	20
4.0 Security classes	20
4.1 Air interface authentication mechanisms	21
4.1.1 Overview	21
4.1.1a Authentication and key management algorithms.....	21
4.1.2 Authentication of an MS.....	21
4.1.3 Authentication of the infrastructure	22
4.1.4 Mutual authentication of MS and infrastructure.....	23
4.1.5 The authentication key.....	25
4.1.6 Equipment authentication	25
4.1.6a Request for information related to an MS.....	26
4.1.7 Authentication of an MS when migrated.....	26
4.1.8 Authentication of the home SWMI when migrated.....	27
4.1.9 Mutual Authentication of MS and infrastructure when migrated.....	28
4.2 Air Interface key management mechanisms.....	29
4.2.0 General.....	29
4.2.1 The DCK.....	29
4.2.2 The GCK.....	30
4.2.2.0 General.....	30
4.2.2.1 Session key modifier GCK0.....	31
4.2.3 The CCK.....	32
4.2.4 The SCK	33
4.2.4.0 General	33
4.2.4.1 SCK association for DMO use	35
4.2.4.1.0 General	35
4.2.4.1.1 DMO SCK subset grouping.....	35
4.2.5 The GSKO	37
4.2.5.0 General	37
4.2.5.1 SCK distribution to groups with OTAR.....	38
4.2.5.2 GCK distribution to groups with OTAR	38
4.2.5.3 Rules for MS response to group key distribution.....	39
4.2.6 Encrypted Short Identity (ESI) mechanism	39
4.2.7 Encryption Cipher Key	40
4.2.8 Summary of AI key management mechanisms.....	40
4.3 Service description and primitives	42
4.3.1 Authentication primitives	42
4.3.2 SCK transfer primitives	42
4.3.3 GCK transfer primitives.....	43
4.3.4 GSKO transfer primitives	44
4.4 Authentication protocol.....	45
4.4.1 Authentication state transitions.....	45
4.4.2 Authentication protocol sequences and operations.....	48
4.4.2.0 General	48
4.4.2.1 MSCs for authentication	49

4.4.2.2	MSCs for authentication and security type-3 elements	55
4.4.2.3	Control of authentication timer T354 at MS	58
4.4a	Information request protocol	59
4.5	OTAR protocols	62
4.5.1	CCK delivery - protocol functions	62
4.5.1.0	General	62
4.5.1.1	SwMI-initiated CCK provision	63
4.5.1.2	MS-initiated CCK provision with U-OTAR CCK demand	65
4.5.1.3	MS-initiated CCK provision with announced cell reselection	65
4.5.2	OTAR protocol functions - SCK	66
4.5.2.0	General	66
4.5.2.1	MS requests provision of SCK(s)	67
4.5.2.2	SwMI provides SCK(s) to individual MS	68
4.5.2.3	SwMI provides SCK(s) to group of MSs	70
4.5.2.4	SwMI rejects provision of SCK	71
4.5.3	OTAR protocol functions - GCK	72
4.5.3.0	General	72
4.5.3.1	MS requests provision of GCK	72
4.5.3.2	SwMI provides GCK to an individual MS	74
4.5.3.3	SwMI provides GCK to a group of MSs	75
4.5.3.4	SwMI rejects provision of GCK	77
4.5.4	Cipher key association to group address	78
4.5.4.0	General	78
4.5.4.1	SCK association for DMO	79
4.5.4.2	GCK association	82
4.5.5	Notification of key change over the air	84
4.5.5.0	General	84
4.5.5.1	Change of DCK	85
4.5.5.2	Change of CCK	86
4.5.5.3	Change of GCK	86
4.5.5.4	Change of SCK for TMO	86
4.5.5.5	Change of SCK for DMO	86
4.5.5.6	Synchronization of Cipher Key Change	87
4.5.6	Security class change	87
4.5.6.0	General	87
4.5.6.1	Change of security class to security class 1	88
4.5.6.2	Change of security class to security class 2	88
4.5.6.3	Change of security class to security class 3	88
4.5.6.4	Change of security class to security class 3 with GCK	88
4.5.7	Notification of key in use	89
4.5.8	Notification of GCK Activation/Deactivation	89
4.5.9	Deletion of SCK, GCK and GSKO	89
4.5.10	Air Interface Key Status Enquiry	91
4.5.11	Crypto management group	93
4.5.12	OTAR retry mechanism	94
4.5.13	OTAR protocol functions - GSKO	94
4.5.13.0	General	94
4.5.13.1	MS requests provision of GSKO	95
4.5.13.2	SwMI provides GSKO to an MS	95
4.5.13.3	SwMI rejects provision of GSKO	96
4.5.14	OTAR protocol functions - interaction and queuing	96
4.5.15	KSOv for OTAR operations in visited SwMI	96
4.5.16	Transfer of AI cipher keys across the ISI	100
5	Enable and disable mechanism	100
5.0	General	100
5.1	General relationships	101
5.2	Enable/disable state transitions	101
5.3	Mechanisms	102
5.3.0	General	102
5.3.1	Disable of MS equipment	103
5.3.2	Disable of an subscription	103

5.3.3	Disable of subscription and equipment	103
5.3.4	Enable an MS equipment	103
5.3.5	Enable an MS subscription	103
5.3.6	Enable an MS equipment and subscription	103
5.4	Enable/disable protocol	104
5.4.1	General case	104
5.4.2	Status of cipher key material	105
5.4.2.1	Permanently disabled state	105
5.4.2.2	Temporarily disabled state	105
5.4.3	Specific protocol exchanges	106
5.4.3.0	General	106
5.4.3.1	Disabling an MS with mutual authentication	106
5.4.3.2	Enabling an MS with mutual authentication	107
5.4.3.3	Enabling an MS with non-mutual authentication	108
5.4.3.4	Disabling an MS with non-mutual authentication	110
5.4.4	Enabling an MS without authentication	111
5.4.5	Disabling an MS without authentication	111
5.4.6	Rejection of enable or disable command	111
5.4.6a	Expiry of Enable/Disable protocol timer	112
5.4.7	MM service primitives	112
5.4.7.0	General	112
5.4.7.1	TNMM-DISABLING primitive	113
5.4.7.2	TNMM-ENABLING primitive	113
6	Air Interface (AI) encryption	113
6.1	General principles	113
6.2	Security class	114
6.2.a	General	114
6.2.0	Notification of security class	115
6.2.0.0	General	115
6.2.0.1	Security Class of Neighbouring Cells	116
6.2.0.2	Identification of MS security capabilities	116
6.2.1	Constraints on LA arising from cell class	116
6.3	Key Stream Generator (KSG)	116
6.3.0	General	116
6.3.1	KSG numbering and selection	117
6.3.2	Interface parameters	117
6.3.2.1	Initial Value (IV)	117
6.3.2.2	Cipher Key	118
6.4	Encryption mechanism	118
6.4.0	General	118
6.4.1	Allocation of KSS to logical channels	118
6.4.2	Allocation of KSS to logical channels with PDU association	120
6.4.2.1	General	120
6.4.2.2	KSS allocation on phase modulation channels	121
6.4.2.3	KSS allocation on QAM channels	122
6.4.2.3.0	General	122
6.4.2.3.1	Fixed mapping	122
6.4.2.3.2	Offset mapping	123
6.4.3	Synchronization of data calls where data is multi-slot interleaved	124
6.4.4	Recovery of stolen frames from interleaved data	125
6.5	Use of cipher keys	126
6.5.0	General	126
6.5.1	Identification of encryption state of downlink MAC PDUs	127
6.5.1.0	General	127
6.5.1.1	Class 1 cells	127
6.5.1.2	Class 2 cells	128
6.5.1.3	Class 3 cells	128
6.5.2	Identification of encryption state of uplink MAC PDUs	128
6.6	Mobility procedures	129
6.6.1	General requirements	129
6.6.1.0	Common requirements	129

6.6.1.1	Additional requirements for class 3 systems	129
6.6.2	Protocol description	129
6.6.2.0	General	129
6.6.2.1	Negotiation of ciphering parameters	129
6.6.2.1.0	General	129
6.6.2.1.1	Class 1 cells	130
6.6.2.1.2	Class 2 cells	130
6.6.2.1.3	Class 3 cells	130
6.6.2.2	Initial and undeclared cell re-selection	130
6.6.2.3	Unannounced cell re-selection	131
6.6.2.4	Announced cell re-selection type-3	132
6.6.2.5	Announced cell re-selection type-2	132
6.6.2.6	Announced cell re-selection type-1	132
6.6.2.7	Key forwarding	132
6.6.3	Shared channels	133
6.7	Encryption control	134
6.7.0	General	134
6.7.1	Data to be encrypted	134
6.7.1.1	Downlink control channel requirements	134
6.7.1.2	Encryption of MAC header elements	134
6.7.1.3	Traffic channel encryption control	134
6.7.1.4	Handling of PDUs that do not conform to negotiated ciphering mode	135
6.7.2	Service description and primitives	135
6.7.2.0	General	135
6.7.2.1	Mobility Management (MM)	136
6.7.2.2	Mobile Link Entity (MLE)	137
6.7.2.3	Layer 2	139
6.7.3	Protocol functions	139
6.7.3.0	General	139
6.7.3.1	MM	139
6.7.3.2	MLE	139
6.7.3.3	LLC	139
6.7.3.4	MAC	140
6.7.4	PDUs for cipher negotiation	140

Annex A (normative): PDU and element definitions141

A.0	General	141
A.1	Authentication PDUs	141
A.1.1	D-AUTHENTICATION demand	141
A.1.2	D-AUTHENTICATION reject	141
A.1.3	D-AUTHENTICATION response	142
A.1.4	D-AUTHENTICATION result	142
A.1.5	U-AUTHENTICATION demand	142
A.1.6	U-AUTHENTICATION reject	143
A.1.7	U-AUTHENTICATION response	143
A.1.8	U-AUTHENTICATION result	144
A.2	OTAR PDUs	144
A.2.1	D-OTAR CCK Provide	144
A.2.2	U-OTAR CCK Demand	144
A.2.3	D-OTAR CCK Result	145
A.2.4	D-OTAR GCK Provide	145
A.2.5	U-OTAR GCK Demand	146
A.2.6	U-OTAR GCK Result	147
A.2.6a	D-OTAR GCK Reject	147
A.2.7	D-OTAR SCK Provide	148
A.2.8	U-OTAR SCK Demand	149
A.2.9	U-OTAR SCK Result	149
A.2.9a	D-OTAR SCK Reject	150
A.2.10	D-OTAR GSKO Provide	150
A.2.11	U-OTAR GSKO Demand	151

A.2.12	U-OTAR GSKO Result.....	151
A.2.12a	D-OTAR GSKO Reject.....	151
A.3	PDU for key association to GTSI.....	152
A.3.1	D-OTAR KEY ASSOCIATE demand.....	152
A.3.2	U-OTAR KEY ASSOCIATE status.....	153
A.4	PDU to synchronize key or security class change.....	153
A.4.1	D-CK CHANGE demand.....	153
A.4.2	U-CK CHANGE result.....	154
A.4.2a	U-OTAR KEY DELETE result.....	155
A.4.2b	U-OTAR KEY STATUS response.....	156
A.4.3	D-DM-SCK ACTIVATE DEMAND.....	157
A.4.4	U-DM-SCK ACTIVATE RESULT.....	158
A.4a	PDU to delete air interface keys in MS.....	159
A.4a.1	D-OTAR KEY DELETE demand.....	159
A.4a.2	U-OTAR KEY DELETE result.....	159
A.4b	PDU to obtain Air Interface Key Status.....	160
A.4b.1	D-OTAR KEY STATUS demand.....	160
A.4b.2	U-OTAR KEY STATUS response.....	161
A.5	Other security domain PDUs.....	162
A.5.1	U-TEI PROVIDE.....	162
A.5.2	U-OTAR PREPARE.....	163
A.5.3	D-OTAR NEWCELL.....	163
A.5.4	D-OTAR CMG GTSI PROVIDE.....	163
A.5.5	U-OTAR CMG GTSI RESULT.....	164
A.5.6	U-INFORMATION PROVIDE.....	164
A.6	PDU for Enable and Disable.....	166
A.6.1	D-DISABLE.....	166
A.6.2	D-ENABLE.....	166
A.6.3	U-DISABLE STATUS.....	167
A.7	MM PDU type 3 information elements coding.....	167
A.7.0	General.....	167
A.7.1	Authentication downlink.....	167
A.7.2	Authentication uplink.....	168
A.7.3	Security downlink.....	168
A.8	PDU Information elements coding.....	169
A.8.0	General.....	169
A.8.1	Acknowledgement flag.....	169
A.8.1a	Additional information present.....	169
A.8.2	Address extension.....	169
A.8.2a	AI algorithm information present.....	169
A.8.2b	AI algorithm information request flag.....	170
A.8.3	Authentication challenge.....	170
A.8.4	Authentication reject reason.....	170
A.8.5	Authentication result.....	170
A.8.6	Authentication sub-type.....	170
A.8.7	CCK identifier.....	171
A.8.8	CCK information.....	171
A.8.9	CCK Location area information.....	171
A.8.10	CCK request flag.....	172
A.8.11	Change of security class.....	172
A.8.12	Ciphering parameters.....	172
A.8.13	CK provision flag.....	173
A.8.14	CK provisioning information.....	173
A.8.15	CK request flag.....	173
A.8.16	Class Change flag.....	173
A.8.17	DCK forwarding result.....	173
A.8.18	Disabling type.....	174

A.8.19	Enable/Disable result.....	174
A.8.20	Encryption mode	174
A.8.20.1	Class 1 cells	174
A.8.20.2	Class 2 cells	175
A.8.20.3	Class 3 cells	175
A.8.21	Equipment disable	175
A.8.22	Equipment enable	175
A.8.23	Equipment status	175
A.8.23a	Explicit response	176
A.8.24	Frame number	176
A.8.24a	Future information present	176
A.8.25	Future key flag	176
A.8.26	GCK data.....	177
A.8.27	GCK key and identifier	177
A.8.28	GCK Number (GCKN)	177
A.8.28a	GCK Provision result	177
A.8.28b	GCK rejected.....	178
A.8.29	GCK select number	178
A.8.29a	GCK Supported.....	178
A.8.30	GCK Version Number (GCK-VN).....	178
A.8.31	Group association	179
A.8.31a	Group Identity Security Related Information	179
A.8.32	GSKO Version Number (GSKO-VN).....	179
A.8.33	GSSI	179
A.8.33a	HW SW version request flag	180
A.8.33b	HW version number present.....	180
A.8.34	Hyperframe number	180
A.8.35	Intent/confirm.....	180
A.8.36	Void.....	180
A.8.37	Key association status	180
A.8.38	Key association type.....	181
A.8.39	Key change type	181
A.8.39a	Key delete type	181
A.8.39b	Key status type	181
A.8.39c	Key delete extension	182
A.8.40	Key type flag	182
A.8.41	KSG-number	182
A.8.42	Location area	182
A.8.43	Location area bit mask	183
A.8.44	Location area selector.....	183
A.8.45	Location area list	183
A.8.46	Location area range	183
A.8.46a	Max response timer value.....	183
A.8.47	Mobile country code.....	184
A.8.48	Mobile network code.....	184
A.8.48a	Model number information present	184
A.8.48b	Model number request flag.....	184
A.8.49	Multiframe number.....	184
A.8.50	Mutual authentication flag.....	184
A.8.51	Network time.....	185
A.8.52	Number of GCKs changed	185
A.8.52a	Number of GCKs deleted	185
A.8.52b	Number of GCK status	185
A.8.52c	Number of GCKs provided	185
A.8.52d	Number of GCKs rejected.....	186
A.8.52e	Number of GCKs requested by GCKN	186
A.8.52f	Number of GCKs requested by GSSI.....	187
A.8.53	Number of groups.....	187
A.8.53a	Number of GSKO status.....	187
A.8.53b	Number of KSGs present	187
A.8.54	Number of location areas	188
A.8.55	Number of SCKs changed.....	188

A.8.55a	Number of SCKs deleted.....	188
A.8.56	Number of SCKs provided.....	188
A.8.56a	Number of SCKs rejected.....	189
A.8.57	Number of SCKs requested.....	189
A.8.57a	Number of SCK status.....	189
A.8.57b	OTAR reject reason.....	190
A.8.57c	OTAR retry interval.....	190
A.8.58	OTAR sub-type.....	190
A.8.59	PDU type.....	191
A.8.60	Proprietary.....	192
A.8.61	Provision result.....	192
A.8.62	Random challenge.....	192
A.8.63	Random seed.....	192
A.8.64	Random seed for OTAR.....	192
A.8.65	Void.....	193
A.8.65a	Reject reason.....	193
A.8.66	Response value.....	193
A.8.67	SCK data.....	193
A.8.68	SCK information.....	193
A.8.69	SCK key and identifier.....	194
A.8.70	SCK Number (SCKN).....	194
A.8.71	SCK number and result.....	194
A.8.72	SCK provision flag.....	194
A.8.72a	Void.....	195
A.8.72b	SCK rejected.....	195
A.8.73	SCK select number.....	195
A.8.73a	SCK subset grouping type.....	195
A.8.73b	SCK subset number.....	196
A.8.74	SCK use.....	196
A.8.75	SCK version number.....	196
A.8.76	Sealed Key (Sealed CCK, Sealed SCK, Sealed GCK, Sealed GSKO).....	196
A.8.77	Security information element.....	197
A.8.77a	Security parameters.....	198
A.8.77b	Security related information element.....	198
A.8.78	Session key.....	198
A.8.79	Slot Number.....	199
A.8.80	SSI.....	199
A.8.81	Subscription disable.....	199
A.8.82	Subscription enable.....	199
A.8.83	Subscription status.....	199
A.8.83a	SW version number present.....	200
A.8.84	TEI.....	200
A.8.85	TEI request flag.....	200
A.8.86	Time type.....	200
A.8.87	Type 3 element identifier.....	201

Annex B (normative): Boundary conditions for the cryptographic algorithms and procedures202

B.0	General.....	202
B.1	Dimensioning of the cryptographic parameters.....	207
B.2	Summary of the cryptographic processes.....	208

Annex C (normative): Timers213

C.1	T354, authentication protocol timer.....	213
C.2	T371, Delay timer for group addressed delivery of SCK and GCK.....	213
C.3	T372, Key forwarding timer.....	213
C.4	T355, disable control timer.....	213

Annex D (informative):	Bibliography.....	214
Annex E (informative):	Change request history.....	215
History		216

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Full standard:
<https://standards.iteh.ai/catalog/standards/sist/5c6262c7-b05-4685-a9bc-3bb5c4641eb8/etsi-en-300-392-7-v3.4.1-2017-01>

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 (<https://ipr.etsi.org/>).

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 European Standard (EN) 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 Voice plus Data (V+D), as identified below:

- ETSI EN 300 392-1: "General network design";
- ETSI EN 300 392-2: "Air Interface (AI)";
- ETSI EN 300 392-3: "Interworking at the Inter-System Interface (ISI)";
- ETSI ETS 300 392-4: "Gateways basic operation";
- ETSI EN 300 392-5: "Peripheral Equipment Interface (PEI)";
- ETSI EN 300 392-7: "Security";**
- ETSI EN 300 392-9: "General requirements for supplementary services";
- ETSI EN 300 392-10: "Supplementary services stage 1";
- ETSI EN 300 392-11: "Supplementary services stage 2";
- ETSI EN 300 392-12: "Supplementary services stage 3";
- ETSI ETS 300 392-13: "SDL model of the Air Interface (AI)";
- ETSI ETS 300 392-14: "Protocol Implementation Conformance Statement (PICS) proforma specification";
- ETSI TS 100 392-15: "TETRA frequency bands, duplex spacings and channel numbering";
- ETSI TS 100 392-16: "Network Performance Metrics";
- ETSI TR 100 392-17: "TETRA V+D and DMO specifications";
- ETSI TS 100 392-18: "Air interface optimized applications".

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 100 392-2 and those may be the latest version of the document.

National transposition dates	
Date of adoption of this EN:	27 December 2016
Date of latest announcement of this EN (doa):	31 March 2017
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	30 September 2017
Date of withdrawal of any conflicting National Standard (dow):	30 September 2017

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)
 Full standard:
<https://standards.iteh.ai/catalog/standards/sist/5c6262c7-b05-4685-a9bc-3bb5c4641eb8/etsi-en-300-392-7-v3.4.1-2017-01>

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 two 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.

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.

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.

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

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 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".