

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

---

**iTeh STANDARD PREVIEW**  
(standards.iteh.ai)

Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/3ef5cbac-17f5-4e8-9d48-60afe803888c/etsi-en-300-392-7-v3.1.1-2008-06>



---

Reference

REN/TETRA-06173

---

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**

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](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.  
All rights reserved.

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

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

# Contents

Intellectual Property Rights .....	9
Foreword.....	9
1 Scope .....	11
2 References .....	11
2.1 Normative references .....	12
2.2 Informative references.....	12
3 Definitions and abbreviations.....	12
3.1 Definitions .....	12
3.2 Abbreviations .....	15
4 Air Interface authentication and key management mechanisms .....	16
4.0 Security classes .....	17
4.1 Air interface authentication mechanisms .....	17
4.1.1 Overview .....	17
4.1.2 Authentication of an MS.....	18
4.1.3 Authentication of the infrastructure .....	18
4.1.4 Mutual authentication of MS and infrastructure .....	19
4.1.5 The authentication key.....	21
4.1.6 Equipment authentication .....	21
4.2 Air Interface key management mechanisms.....	22
4.2.1 The DCK.....	22
4.2.2 The GCK.....	23
4.2.3 The CCK.....	24
4.2.4 The SCK .....	25
4.2.4.1 SCK association for DMO use .....	26
4.2.4.1.1 DMO SCK subset grouping.....	26
4.2.5 The GSKO .....	29
4.2.5.1 SCK distribution to groups with OTAR.....	29
4.2.5.2 GCK distribution to groups with OTAR.....	29
4.2.5.3 Rules for MS response to group key distribution.....	30
4.2.6 Encrypted Short Identity (ESI) mechanism .....	30
4.2.7 Encryption Cipher Key .....	31
4.2.8 Summary of AI key management mechanisms.....	31
4.3 Service description and primitives .....	32
4.3.1 Authentication primitives .....	32
4.3.2 SCK transfer primitives .....	33
4.3.3 GCK transfer primitives.....	34
4.3.4 GSKO transfer primitives .....	35
4.4 Authentication protocol.....	35
4.4.1 Authentication state transitions.....	35
4.4.2 Authentication protocol sequences and operations .....	38
4.4.2.1 MSCs for authentication .....	39
4.4.2.2 MSCs for authentication Type-3 element .....	45
4.4.2.3 Control of authentication timer T354 at MS .....	48
4.5 OTAR protocols .....	49
4.5.1 CCK delivery - protocol functions.....	49
4.5.1.1 SwMI-initiated CCK provision .....	49
4.5.1.2 MS-initiated CCK provision with U-OTAR CCK demand.....	51
4.5.1.3 MS-initiated CCK provision with announced cell reselection .....	52
4.5.2 OTAR protocol functions - SCK .....	52
4.5.2.1 MS requests provision of SCK(s).....	53
4.5.2.2 SwMI provides SCK(s) to individual MS .....	54
4.5.2.3 SwMI provides SCK(s) to group of MSs .....	56
4.5.2.4 SwMI rejects provision of SCK .....	58
4.5.3 OTAR protocol functions - GCK.....	58
4.5.3.1 MS requests provision of GCK .....	58

4.5.3.2	SwMI provides GCK to an individual MS	61
4.5.3.3	SwMI provides GCK to a group of MSs	63
4.5.3.4	SwMI rejects provision of GCK	65
4.5.4	Cipher key association to group address	65
4.5.4.1	SCK association for DMO	66
4.5.4.2	GCK association	69
4.5.5	Notification of key change over the air	71
4.5.5.1	Change of DCK	73
4.5.5.2	Change of CCK	73
4.5.5.3	Change of GCK	73
4.5.5.4	Change of SCK for TMO	73
4.5.5.5	Change of SCK for DMO	74
4.5.5.6	Synchronization of Cipher Key Change	74
4.5.6	Security class change	74
4.5.6.1	Change of security class to security class 1	75
4.5.6.2	Change of security class to security class 2	75
4.5.6.3	Change of security class to security class 3	75
4.5.6.4	Change of security class to security class 3 with GCK	76
4.5.7	Notification of key in use	76
4.5.8	Notification of GCK Activation/Deactivation	76
4.5.9	Deletion of SCK, GCK and GSKO	76
4.5.10	Air Interface Key Status Enquiry	78
4.5.11	Crypto management group	80
4.5.12	OTAR retry mechanism	81
4.5.13	OTAR protocol functions – GSKO	81
4.5.13.1	MS requests provision of GSKO	81
4.5.13.2	SwMI provides GSKO to an MS	82
4.5.13.3	SwMI rejects provision of GSKO	83
5	Enable and disable mechanism	83
5.1	General relationships	83
5.2	Enable/disable state transitions	84
5.3	Mechanisms	84
5.3.1	Disable of MS equipment	85
5.3.2	Disable of an subscription	85
5.3.3	Disable of subscription and equipment	85
5.3.4	Enable an MS equipment	85
5.3.5	Enable an MS subscription	85
5.3.6	Enable an MS equipment and subscription	85
5.4	Enable/disable protocol	86
5.4.1	General case	86
5.4.2	Status of cipher key material	87
5.4.2.1	Permanently disabled state	87
5.4.2.2	Temporarily disabled state	87
5.4.3	Specific protocol exchanges	88
5.4.3.1	Disabling an MS with mutual authentication	88
5.4.3.2	Enabling an MS with mutual authentication	89
5.4.3.3	Enabling an MS with non-mutual authentication	90
5.4.3.4	Disabling an MS with non-mutual authentication	91
5.4.4	Enabling an MS without authentication	93
5.4.5	Disabling an MS without authentication	94
5.4.6	Rejection of enable or disable command	94
5.4.6a	Expiry of Enable/Disable protocol timer	95
5.4.7	MM service primitives	95
5.4.7.1	TNMM-DISABLING primitive	96
5.4.7.2	TNMM-ENABLING primitive	96
6	Air Interface (AI) encryption	96
6.1	General principles	96
6.2	Security class	97
6.2.0	Notification of security class	98
6.2.0.1	Security Class of Neighbouring Cells	98

6.2.0.2	Identification of MS security capabilities .....	99
6.2.1	Constraints on LA arising from cell class .....	99
6.3	Key Stream Generator (KSG) .....	99
6.3.1	KSG numbering and selection .....	99
6.3.2	Interface parameters .....	100
6.3.2.1	Initial Value (IV) .....	100
6.3.2.2	Cipher Key .....	100
6.4	Encryption mechanism .....	101
6.4.1	Allocation of KSS to logical channels .....	101
6.4.2	Allocation of KSS to logical channels with PDU association .....	103
6.4.2.1	General .....	103
6.4.2.2	KSS allocation on phase modulation channels .....	103
6.4.2.3	KSS allocation on QAM channels .....	105
6.4.2.3.1	Fixed mapping .....	105
6.4.2.3.2	Offset mapping .....	106
6.4.3	Synchronization of data calls where data is multi-slot interleaved .....	107
6.4.4	Recovery of stolen frames from interleaved data .....	108
6.5	Use of cipher keys .....	108
6.5.1	Identification of encryption state of downlink MAC PDUs .....	109
6.5.1.1	Class 1 cells .....	109
6.5.1.2	Class 2 cells .....	110
6.5.1.3	Class 3 cells .....	110
6.5.2	Identification of encryption state of uplink MAC PDUs .....	110
6.6	Mobility procedures .....	111
6.6.1	General requirements .....	111
6.6.1.1	Additional requirements for class 3 systems .....	111
6.6.2	Protocol description .....	111
6.6.2.1	Negotiation of cipher parameters .....	111
6.6.2.1.1	Class 1 cells .....	112
6.6.2.1.2	Class 2 cells .....	112
6.6.2.1.3	Class 3 cells .....	112
6.6.2.2	Initial and undeclared cell re-selection .....	112
6.6.2.3	Unannounced cell re-selection .....	113
6.6.2.4	Announced cell re-selection type-3 .....	114
6.6.2.5	Announced cell re-selection type-2 .....	114
6.6.2.6	Announced cell re-selection type-1 .....	114
6.6.2.7	Key forwarding .....	114
6.7	Encryption control .....	116
6.7.1	Data to be encrypted .....	116
6.7.1.1	Downlink control channel requirements .....	116
6.7.1.2	Encryption of MAC header elements .....	116
6.7.1.3	Traffic channel encryption control .....	116
6.7.1.4	Handling of PDUs that do not conform to negotiated ciphering mode .....	117
6.7.2	Service description and primitives .....	117
6.7.2.1	Mobility Management (MM) .....	118
6.7.2.2	Mobile Link Entity (MLE) .....	118
6.7.2.3	Layer 2 .....	120
6.7.3	Protocol functions .....	120
6.7.3.1	MM .....	120
6.7.3.2	MLE .....	120
6.7.3.3	LLC .....	120
6.7.3.4	MAC .....	121
6.7.4	PDUs for cipher negotiation .....	121
<b>Annex A (normative): PDU and element definitions .....</b>		<b>122</b>
A.1	Authentication PDUs .....	122
A.1.1	D-AUTHENTICATION demand .....	122
A.1.2	D-AUTHENTICATION reject .....	122
A.1.3	D-AUTHENTICATION response .....	123
A.1.4	D-AUTHENTICATION result .....	123
A.1.5	U-AUTHENTICATION demand .....	123

A.1.6	U-AUTHENTICATION reject.....	124
A.1.7	U-AUTHENTICATION response.....	124
A.1.8	U-AUTHENTICATION result.....	125
A.2	OTAR PDUs .....	125
A.2.1	D-OTAR CCK Provide .....	125
A.2.2	U-OTAR CCK Demand .....	125
A.2.3	U-OTAR CCK Result .....	126
A.2.4	D-OTAR GCK Provide .....	126
A.2.5	U-OTAR GCK Demand .....	127
A.2.6	U-OTAR GCK Result .....	128
A.2.6a	D-OTAR GCK Reject .....	128
A.2.7	D-OTAR SCK Provide.....	129
A.2.8	U-OTAR SCK Demand.....	130
A.2.9	U-OTAR SCK Result.....	130
A.2.9a	D-OTAR SCK Reject.....	131
A.2.10	D-OTAR GSKO Provide.....	131
A.2.11	U-OTAR GSKO Demand .....	132
A.2.12	U-OTAR GSKO Result.....	132
A.2.12a	D-OTAR GSKO Reject.....	132
A.3	PDUs for key association to GTSI .....	133
A.3.1	D-OTAR KEY ASSOCIATE demand .....	133
A.3.2	U-OTAR KEY ASSOCIATE status.....	134
A.4	PDUs to synchronize key or security class change .....	134
A.4.1	D-CK CHANGE demand.....	134
A.4.2	U-CK CHANGE result.....	135
A.4a	PDUs to delete air interface keys in MS .....	136
A.4a.1	D-OTAR KEY DELETE demand .....	136
A.4a.2	U-OTAR KEY DELETE result.....	137
A.4b	PDUs to obtain Air Interface Key Status .....	138
A.4b.1	D-OTAR KEY STATUS demand.....	138
A.4b.2	U-OTAR KEY STATUS response.....	139
A.5	Other security domain PDUs.....	140
A.5.1	U-TEI PROVIDE .....	140
A.5.2	U-OTAR PREPARE .....	141
A.5.3	D-OTAR NEWCELL.....	141
A.5.4	D-OTAR CMG GTSI PROVIDE.....	141
A.5.5	U-OTAR CMG GTSI RESULT .....	142
A.6	PDUs for Enable and Disable.....	142
A.6.1	D-DISABLE.....	142
A.6.2	D-ENABLE.....	143
A.6.3	U-DISABLE STATUS .....	143
A.7	MM PDU type 3 information elements coding .....	144
A.7.1	Authentication downlink .....	144
A.7.2	Authentication uplink .....	144
A.8	PDU Information elements coding.....	145
A.8.1	Acknowledgement flag.....	145
A.8.2	Address extension.....	145
A.8.3	Authentication challenge .....	145
A.8.4	Authentication reject reason .....	145
A.8.5	Authentication result .....	146
A.8.6	Authentication sub-type .....	146
A.8.7	CCK identifier .....	146
A.8.8	CCK information.....	146
A.8.9	CCK Location area information .....	147
A.8.10	CCK request flag .....	147
A.8.11	Change of security class .....	147
A.8.12	Cipher parameters.....	147

A.8.13	CK provision flag .....	148
A.8.14	CK provisioning information .....	148
A.8.15	CK request flag .....	148
A.8.16	Class Change flag .....	149
A.8.17	DCK forwarding result .....	149
A.8.18	Disabling type .....	149
A.8.19	Enable/Disable result .....	149
A.8.20	Encryption mode .....	150
A.8.20.1	Class 1 cells .....	150
A.8.20.2	Class 2 cells .....	150
A.8.20.3	Class 3 cells .....	150
A.8.21	Equipment disable .....	150
A.8.22	Equipment enable .....	151
A.8.23	Equipment status .....	151
A.8.23a	Explicit response .....	151
A.8.24	Frame number .....	151
A.8.25	Future key flag .....	151
A.8.26	GCK data .....	152
A.8.27	GCK key and identifier .....	152
A.8.28	GCK Number (GCKN) .....	152
A.8.28a	GCK Provision result .....	152
A.8.28b	GCK rejected .....	153
A.8.29	GCK select number .....	153
A.8.29a	GCK Supported .....	153
A.8.30	GCK Version Number (GCK-VN) .....	153
A.8.31	Group association .....	154
A.8.31a	Group Identity Security Related Information .....	154
A.8.32	GSKO Version Number (GSKO-VN) .....	154
A.8.33	GSSI .....	154
A.8.34	Hyperframe number .....	154
A.8.35	Intent/confirm .....	154
A.8.36	Void .....	155
A.8.37	Key association status .....	155
A.8.38	Key association type .....	155
A.8.39	Key change type .....	155
A.8.39a	Key delete type .....	156
A.8.39b	Key status type .....	156
A.8.40	Key type flag .....	156
A.8.41	KSG-number .....	157
A.8.42	Location area .....	157
A.8.43	Location area bit mask .....	157
A.8.44	Location area selector .....	157
A.8.45	Location area list .....	157
A.8.46	Location area range .....	158
A.8.46a	Max response timer value .....	158
A.8.47	Mobile country code .....	158
A.8.48	Mobile network code .....	158
A.8.49	Multiframe number .....	158
A.8.50	Mutual authentication flag .....	158
A.8.51	Network time .....	158
A.8.52	Number of GCKs changed .....	159
A.8.52a	Number of GCKs deleted .....	159
A.8.52b	Number of GCK status .....	159
A.8.52c	Number of GCKs provided .....	159
A.8.52d	Number of GCKs rejected .....	160
A.8.52e	Number of GCKs requested by GCKN .....	160
A.8.52f	Number of GCKs requested by GSSI .....	160
A.8.53	Number of groups .....	161
A.8.53a	Number of GSKO status .....	161
A.8.54	Number of location areas .....	161
A.8.55	Number of SCKs changed .....	161
A.8.55a	Number of SCKs deleted .....	162

A.8.56	Number of SCKs provided .....	162
A.8.56a	Number of SCKs rejected.....	162
A.8.57	Number of SCKs requested .....	163
A.8.57a	Number of SCK status.....	163
A.8.57b	OTAR reject reason.....	163
A.8.57c	OTAR retry interval .....	164
A.8.58	OTAR sub-type .....	164
A.8.59	PDU type.....	165
A.8.60	Proprietary .....	165
A.8.61	Provision result.....	165
A.8.62	Random challenge .....	165
A.8.63	Random seed .....	166
A.8.64	Random seed for OTAR.....	166
A.8.65	Void.....	166
A.8.66	Response value .....	166
A.8.67	SCK data .....	166
A.8.68	SCK information .....	167
A.8.69	SCK key and identifier .....	167
A.8.70	SCK Number (SCKN).....	167
A.8.71	SCK number and result .....	168
A.8.72	SCK provision flag .....	168
A.8.72a	Void.....	168
A.8.72b	SCK rejected .....	168
A.8.73	SCK select number .....	168
A.8.73a	SCK subset grouping type .....	169
A.8.73b	SCK subset number .....	169
A.8.74	SCK use.....	169
A.8.75	SCK version number .....	170
A.8.76	Sealed Key (Sealed CCK, Sealed SCK, Sealed GCK, Sealed GSKO).....	170
A.8.77	Security information element .....	170
A.8.77a	Security related information element.....	171
A.8.78	Session key .....	171
A.8.79	Slot Number .....	171
A.8.80	SSI .....	171
A.8.81	Subscription disable .....	172
A.8.82	Subscription enable .....	172
A.8.83	Subscription status.....	172
A.8.84	TEI.....	172
A.8.85	TEI request flag .....	173
A.8.85a	Timeshare cell and AI encryption information.....	173
A.8.86	Time type.....	173
A.8.87	Type 3 element identifier .....	174

**Annex B (normative):      Boundary conditions for the cryptographic algorithms and procedures .....** **175**

B.1	Dimensioning of the cryptographic parameters .....	180
B.2	Summary of the cryptographic processes.....	181

**Annex C (normative):      Timers .....** **183**

C.1	T354, authorization protocol timer.....	183
C.2	T371, Delay timer for group addressed delivery of SCK and GCK.....	183
C.3	T372, Key forwarding timer.....	183
C.4	T355, disable control timer .....	183

**Annex D (informative):      Bibliography.....** **184**

**Annex E (informative):      Change request history.....** **185**

History .....	186
---------------	-----



---

## 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 European Standard (Telecommunications series) has been produced by ETSI Technical Committee Terrestrial Trunked Radio (TETRA), and is now submitted for the Vote phase of the ETSI standards Two-step Approval Procedure.

The present document is part 7 of a multi-part deliverable covering the Voice plus Data (V+D), as identified below:

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

NOTE: 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.

<b>Proposed national transposition dates</b>	
Date of latest announcement of this EN (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

**iTeh STANDARD PREVIEW**  
(standards.iteh.ai)

Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/3ef5cbac-17f5-4c88-9d48-60afe803888c/etsi-en-300-392-7-v3.1.1-2008-06>

---

# 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.

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 ETR 086-3 [10], 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

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.

## 2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

- [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: "Terrestrial Trunked Radio (TETRA); Security aspects; Subscriber Identity Module to Mobile Equipment (SIM-ME) interface".
- [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)".

## 2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

- [8] ETSI ETS 300 392-2 (1996): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".
- [9] ETSI ETS 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".
- [10] ETSI ETR 086-3: "Trans European Trunked Radio (TETRA) systems; Technical requirements specification; Part 3: Security aspects".
- [11] ETSI EN 300 392-7 (V2.3.1): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".
- [12] ETSI EN 300 392-7 (V2.1.1): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

---

## 3 Definitions and abbreviations

### 3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

**Authentication Code (AC):** (short) sequence to be entered by the user into the MS that may be used in addition to the UAK to generate K with algorithm TB3

**authentication Key (K):** primary secret, the knowledge of which has to be demonstrated for authentication

**authentication session:** period between consecutive successful authentication operations

**CCK Identifier (CCK-id):** identification of the key within an LA

**cipher key:** value that is used to determine the transformation of plain text to cipher text in a cryptographic algorithm

**cipher text:** data produced through the use of encipherment

NOTE: The semantic content of the resulting data is not available (see ISO 7498-2 [3]).

**class:** See security class.

**Common Cipher Key (CCK):** cipher key that is generated by the infrastructure to protect group addressed signalling and traffic

NOTE: CCK is also used to protection of SSI identities (ESI) in layer 2.

**Crypto Management Group (CMG):** group of MSs with common key material

**DCK forwarding:** action of the SwMI whereby a DCK that has already been established with an MS is sent to a cell defined by the MS, at the request of the MS

NOTE: The purpose is to allow the MS to subsequently perform reselection to that cell and use encrypted location updating.

**DCK retrieval:** action of the SwMI whereby a DCK that has already been established with an MS is sent to a cell to which the MS location updates, without any previous knowledge that the MS is going to perform location updating to that cell

NOTE: The purpose is to allow the MS to perform encrypted location updating on that cell without any prior forwarding transaction. The SwMI may be able to perform DCK retrieval during initial registration, during cell reselection, or both.

**decipherment:** reversal of a corresponding reversible encipherment

NOTE: See ISO 7498-2 [3].

**Derived Cipher Key (DCK):** key generated during authentication for use in protection of individually addressed signalling and traffic

**encipherment:** cryptographic transformation of data to produce cipher text

NOTE: See ISO 7498-2 [3].

**Encryption Cipher Key (ECK):** cipher key that is used as input to the encryption algorithm

NOTE: This key is derived from one of SCK, DCK, MGCK or CCK and modified using an algorithm by the broadcast data of the serving cell.

**encryption mode:** choice between static (SCK) and dynamic (DCK/CCK) encipherment

**encryption state:** encryption on or off

**end-to-end encryption:** encryption within or at the source end system, with the corresponding decryption occurring only within or at the destination end system

NOTE: Defined in EN 302 109 [6].

**Extended Group Session Key for OTAR (EGSKO):** cipher key used for distribution of keys to groups of MSs

**fallback SCK:** key used by class 3 system when operating in class 2, for example in a fault or fallback situation

**Group Cipher Key (GCK):** cipher key known by the infrastructure and MS to protect group addressed signalling and traffic

NOTE: Not used directly at the air interface but modified by CCK to give a Modified Group Cipher Key (MGCK).