Final draft ETSI EN 300 392-7 V3.0.3 (2008-04)

European Standard (Telecommunications series)

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

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/chaircor/ETSI_support.asp

Copyright Notification

Contents

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.

Proposed national transposition dates	
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

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).