SLOVENSKI STANDARD
SIST EN 300 392-7 V2.1.1:2003

01-december-2003

Prizemni snopovni radio (TETRA) – Govor in podatki (V+D) – 7. del: Varnost

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

Ta slovenski standard je istoveten z: **EN 300 392-7 Version 2.1.1**

ICS:

33.070.10	Prizemni snopovni radio (TETRA)	Terrestrial Trunked Radio (TETRA)

SIST EN 300 392-7 V2.1.1:2003 **en**

ETSI EN 300 392-7 V2.1.1 (2001-02)

European Standard (Telecommunications series)

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

Reference
REN/TETRA-06001-7

Keywords
TETRA, V+D, Security

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://www.etsi.org/tb/status/

If you find errors in the present document, send your comment to:
editor@etsi.fr

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://www.etsi.org/ipr).

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 Project Terrestrial Trunked Radio (TETRA).

The present document had been submitted to Public Enquiry as ETS 300 392-7. During the processing for Vote it was converted into an EN.

The present document is part 7 of a multi-part deliverable covering the Voice plus Data (V+D), 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 6: "Line connected Station (LS)";

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".

National transposition dates	
Date of adoption of this EN:	9 February 2001
Date of latest announcement of this EN (doa):	31 May 2001
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	30 November 2001
Date of withdrawal of any conflicting National Standard (dow):	30 November 2001

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 document 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 end-to-end confidentiality mechanisms between users.

1.1 Security classes

TETRA security is defined in terms of class. Each class has associated features that are mandatory or optional and are summarized in table 1.

Table 1: Summary of Security features in TETRA by class

Class	Authentication	OTAR	Encryption	Enable-Disable	End-to-end
	Clause 4	Clause 4	Clause 6	Clause 5	Clause 7
1	O	-	-	M	O
2	O	O	M	M	O
3	M	M	M	M	O
NOTE: M = Mandatory; O = Optional; - = Does not apply					

The present document describes a system in which all signalling and traffic within that system comply with the same security class. However signalling permits more than one security class to be supported concurrently within an SwMI, and movements between these classes are described in the present document. The SwMI shall control the state of AI encryption.

An MS may support one, several, or all security classes. Each cell may support at any one time one of the following options:

class 1 only;

class 2 only;

class 2 and class 1;

class 3 only; or

class 3 and class 1.

Class 2 and class 3 are not permitted to be supported at the same time in any cell.

1.2 Document layout

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 [4], based on a threat analysis:

- authentication of a user by the TETRA infrastructure;
- authentication of the TETRA infrastructure by a user.

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.

Clause 7 describes the end-to-end confidentiality for V+D. End-to-end confidentiality can be established between two users or a group of users. In clause 7 the logical part of the interface to the encryption mechanism is described. Electrical and physical aspects of this interface are not described, nor are the encryption algorithms and keys for end-to-end confidentiality described.

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

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] ETSI ETS 300 392-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".

[2] ETSI EN 300 392-2 (V2.3.1): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".

[3] ETSI ETS 300 392-7 (1996): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

[4] ETSI ETR 086-3: "Trans European Trunked Radio (TETRA) systems; Technical requirements specification; Part 3: Security aspects".

[5] ISO 7498-2: "Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture".

[6] ETSI ETS 300 395-1: "Terrestrial Trunked Radio (TETRA); Speech codec for full-rate traffic channel; Part 1: General description of speech functions".

[7] ETSI ETS 300 812: "Terrestrial Trunked Radio (TETRA); Security aspects; Subscriber Identity Module to Mobile Equipment (SIM - ME) interface".

[8] ETSI ETS 300 396-6: "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".

[9] ETSI ETS 300 392-2: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".

3 Definitions, symbols 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

CCK Identity (CCK-Id): distributed with the CCK. It serves the identification of the key within an LA and the protection against replay of old keys

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. The semantic content of the resulting data is not available (see ISO 7498-2 [5])

class: see security class

Common Cipher Key (CCK): cipher key that is generated by the infrastructure to protect group addressed signalling and traffic. CCK is also used to protection of SSI identities (ESI) in layer 2

decipherment: reversal of a corresponding reversible encipherment (see ISO 7498-2 [5])

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

derived key: sequence of symbols that controls the KSG inside the end-to-end encryption unit and that is derived from the cipher key

encipherment: cryptographic transformation of data to produce cipher text (see ISO 7498-2 [5])

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

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

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

flywheel: mechanism to keep the KSG in the receiving terminal synchronized with the KSG in the transmitting terminal in case synchronization data is not received correctly

Group Cipher Key (GCK): cipher key known by the infrastructure and MS to protect group addressed signalling and traffic. Not used directly at the air interface but modified by CCK or SCK to give a Modified Group Cipher Key (MGCK)

Group Session Key for OTAR (GSKO): cipher key used to derive EGSKO for the distribution of keys to groups of users

Initialization Value (IV): sequence of symbols that initializes the KSG inside the encryption unit

key stream: pseudo random stream of symbols that is generated by a KSG for encipherment and decipherment

Key Stream Generator (KSG): cryptographic algorithm which produces a stream of binary digits which can be used for encipherment and decipherment. The initial state of the KSG is determined by the initialization value

Key Stream Segment (KSS): key stream of arbitrary length

Location Area id (LA-id): unique identifier within an SwMI of a location area

Manipulation Flag (MF): used to indicate that a sealed cipher key (CCK, SCK or GCK) has been incorrectly recovered

Modified Group Cipher Key (MGCK): cipher key known by the infrastructure and MS to protect group addressed signalling and traffic that is composed algorithmically from either CCK and GCK, or SCK and GCK

Over The Air Re-keying (OTAR): method by which the SwMI can transfer secret keys securely to terminals

Personal Identification Number (PIN): entered by the user into the MS and used to authenticate the user to the MS

plain text: un-encrypted source data. The semantic content is available

proprietary algorithm: algorithm which is the intellectual property of a legal entity

Random Challenge (RAND1, RAND2): random value generated by the infrastructure to authenticate a user or in an MS to authenticate the infrastructure, respectively

Random Seed (RS): random value used to derive a session authentication key from the authentication key

Random seed for OTAR (RSO): random value used to derive a session key for OTAR from a user's authentication key

Registered Area (RA): collection of location areas (LA) to which the MS may perform cell re-selection without need for explicit invocation of the registration protocol

Response (RES1, RES2): value calculated in the MS from RAND1 and the KS to prove the authenticity of a user to the infrastructure or by the infrastructure from RAND2 and the KS' to prove its authenticity to a user, respectively

SCK-set: collective term for the group of 32 SCK associated with each ITSI

Security class 1, 2 or 3: classification of terminal and SwMI encryption and authentication support. Class 1: no encryption, may use authentication; Class 2: SCK encryption, ESI with SCK, may use authentication; Class 3: DCK encryption, ESI with CCK, authentication

Sealed Common Cipher Key (SCCK): common cipher key cryptographically sealed with a particular user's derived cipher key

Sealed Group Cipher Key (SGCK): group cipher key cryptographically sealed with a particular user's derived cipher key

Sealed Static Cipher Key (SSCK): static cipher key cryptographically sealed with a particular user's secret key

Session Authentication Key (KS, KS'): generated from the authentication key and a random seed for authentication. It has a more limited lifetime than the authentication key and can be stored in less secure places and forwarded to visited networks

Session Key for OTAR (KSO): derived from a user's authentication key and a random seed for OTAR. KSO is used to protect the transfer of the Static Cipher Key

Static Cipher Key (SCK): predetermined cipher key that may be used to provide confidentiality in class 2 systems with a corresponding algorithm

Synchronization value: sequence of symbols that is transmitted to the receiving terminal to synchronize the EKSG in the receiving terminal with the EKSG in the transmitting terminal. The sequence may also contain identification of end-to-end encryption algorithm and the used encryption key

synchronous stream cipher: encryption method in which a cipher text symbol completely represents the corresponding plain text symbol. The encryption is based on a key stream that is independent of the cipher text. In order to synchronize the KSGs in the transmitting and the receiving terminal synchronization data is transmitted separately

TETRA algorithm: mathematical description of a cryptographic process used for either of the security processes authentication or encryption