SLOVENSKI STANDARD
SIST ETS 300 392-7:1999

01-julij-1999

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: **ETS 300 392-7 Edition 1**

ICS:

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

SIST ETS 300 392-7:1999 **en**

EUROPEAN
TELECOMMUNICATION
STANDARD

ETS 300 392-7

December 1996

Source: ETSI TC-RES

Reference: DE/RES-06001-7

ICS: 33.060, 33.060.50

Key words: TETRA, V+D, security

Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 4 92 94 42 00 - Fax: +33 4 93 65 47 16

Contents

Foreword

This European Telecommunication Standard (ETS) has been produced by the Radio Equipment and Systems (RES) Technical Committee of the European Telecommunications Standards Institute (ETSI).

This ETS is a multi-part standard and will consist of the following parts:

Part 1: "General network design";

Part 2: "Air Interface (AI)";

Part 3: "Inter-working - Basic Operation", (DE/RES-06001-3);

Part 4: "Gateways for Basic Services", (DE/RES-06001-4);

Part 5: "Terminal equipment interface", (DE/RES-06001-5);

Part 6: "Line connected stations", (DE/RES-06001-6);

Part 7: "Security";

Part 8: "Management services", (DE/RES-06001-8);

Part 9: "Performance objectives", (DE/RES-06001-9);

Part 10: "Supplementary Services (SS) Stage 1";

Part 11: "Supplementary Services (SS) Stage 2";

Part 12: "Supplementary Services (SS) Stage 3";

Part 13: "SDL Model of the Air Interface";

Part 14: "PICS Proforma" (DE/RES-06001-14);

Part 15: "Inter-working - Extended Operations", (DE/RES-06001-15).

Transposition dates	
Date of adoption	22 November 1996
Date of latest announcement of this ETS (doa):	31 March 1997
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	30 September 1997
Date of withdrawal of any conflicting National Standard (dow):	30 September 1997

Blank page

1 Scope

This European Telecommunication Standard (ETS) defines the Trans-European 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.

This 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 end-to-end confidentiality mechanisms between users.

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 [3], 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 a secure 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 for end-to-end confidentiality described.

This part of the ETS 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 this part of the ETS.

2 Normative references

This ETS incorporates by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] ETS 300 392-1: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".

[2] ETS 300 392-2: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".

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

[4] ISO 7498-2: "Information processing systems - Open Systems Interconnection - Basic reference model - Part 2: Security Architecture".

[5] prETS 300 395-1: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Speech codec for full-rate traffic channel; Part 1: General description of speech functions".

[6] prETS 300 395-3: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Speech codec for full-rate traffic channel; Part 3: Specific operating features".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this ETS, the following definitions apply:

Authentication Code (AC): A (short) sequence to be entered by the user into the MS.

Authentication Key (K): The 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 active key and the protection against replay of old keys.

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

cipher text: The data produced through the use of encipherment. The semantic content of the resulting data is not available (see ISO 7498-2 [4]).

Common Cipher Key (CCK): A cipher key that is generated by the infrastructure to protect group addressed signalling and traffic. There is one CCK for each location area.

decipherment: The reversal of a corresponding reversible encipherment (see ISO 7498-2 [4]).

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

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

encipherment: The cryptographic transformation of data to produce cipher text (see ISO 7498-2 [4]).

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

encryption state: Encryption on or off.

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

flywheel: A 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): A long lifetime cipher key generated by the infrastructure to protect group addressed signalling and traffic. Not used directly at the air interface but modified by CCK to give a Modified Group Cipher Key (MGCK). There is one GCK for each GTSI.

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

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

Key Stream Generator (KSG): A 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): A key stream of arbitrary length.

Manipulation Flag (MF): Used to indicate that the CCK has been incorrectly recovered.

Personal Identification Number (PIN): Entered by the user into the MS and used to generate the authentication Key (K) together with the User Authentication Key (UAK).

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

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

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

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

Response (RES1, RES2): A 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: The collective term for the group of 32 SCK associated with each ITSI.

Sealed Common Cipher Key (SCCK): A common cipher key cryptographically sealed with a particular user's derived cipher key. In this form the keys are distributed over the air interface.

Sealed Group Cipher Key (SGCK): A group cipher key cryptographically sealed with a particular user's derived cipher key. In this form the keys are distributed over the air interface.

Sealed Static Cipher Key (SSCK): A static cipher key cryptographically sealed with a particular user's secret key. In this form the keys are distributed over the air interface.

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.

spoofer: An entity attempting to obtain service from or interfere with the operation of the system by impersonation of an authorized system user or system component.

Static Cipher Key (SCK): A predetermined cipher key that may be used if no (successful) authentication has taken place.

synchronization value: A sequence of symbols that is transmitted to the receiving terminal to synchronize the KSG in the receiving terminal with the KSG in the transmitting terminal.

synchronous stream cipher: An 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: The mathematical description of a cryptographic process used for either of the security processes authentication or encryption.

time stamp: Is a sequence of symbols that represents the time of day.

User Authentication Key (UAK): Stored in a (possibly detachable) module within the MS and used to derive the authentication key (with or without a PIN as an additional parameter).

3.2 Abbreviations

For the purposes of this ETS, the following abbreviations apply:

AC	Authentication Code
AI	Air Interface
AS	Alias Stream
AESI	Alias Encrypted Short Identity
ASSI	Alias Short Subscriber Identity
BS	Base Station
CCK	Common Cipher Key
CCK-id	CCK identifier
C-PLANE	Control-PLANE
CT	Cipher Text
DCK	Derived Cipher Key
DCK1	Part 1 of the DCK
DCK2	Part 2 of the DCK
DK	Derived Key
EKSG	End-to-end Key Stream Generator
EKSS	End-to-end Key Stream Segment
ESI	Encrypted Short Identity
F	Function
FEC	Forward Error Correction
GCK	Group Cipher Key
GCK-VN	GCK-Version Number
GESI	Group Encrypted Short Identity
GSSI	Group Short Subscriber Identity
GTSI	Group TETRA Subscriber Identity
HSC	Half-Slot Condition
HSI	Half-Slot Importance
HSN	Half-Slot Number
HSS	Half-Slot Stolen
HSSE	Half-Slot Stolen by Encryption unit
IESI	Individual Encrypted Short Identity
ISSI	Individual Short Subscriber Identity
ITSI	Individual TETRA Subscriber Identity
IV	Initialization Value
K	authentication Key
KS, KS'	Session authentication Key
KSG	Key Stream Generator
KSO	Session Key OTAR
KSS	Key Stream Segment
LA	Location Area
LLC	Logical Link Control
MAC	Medium Access Control
MF	Manipulation Flag
MGCK	Modified Group Cipher Key
MLE	Mobile Link Entity
MM	Mobility Management
MNI	Mobile Network Identity
MS	Mobile Station
MSC	Message Sequence Chart
PDU	Protocol Data Unit
PIN	Personal Identification Number
PT	Plain Text
RAND1	RANDom challenge 1
RAND2	RANDom challenge 2
RES1	RESponse 1
RES2	RESponse 2
RS	Random Seed
RSO	Random Seed for OTAR
SAP	Service Access Point
SCCK	Sealed Common Cipher Key

SCK	Static Cipher Key
SCK-VN	SCK Identifier
SCKN	Static Cipher Key Number
SDU	Service Data Unit
SGCK	Sealed GCK
SHSI	Stolen Half-Slot Identifier
SS	Synchronization Status
SSCK	Sealed SCK
SSI	Short Subscriber Identity
SV	Synchronization Value
SwMI	Switching and Management Infrastructure
TA	TETRA Algorithm
TCH	Traffic Channel type
TEI	TETRA Equipment Identity
TSI	TETRA Subscriber Identity
UAK	User Authentication Key
U-PLANE	User-PLANE
XRES1	eXpected RESponse 1
XRES2	eXpected RESponse 2

4 Air Interface authentication and key management mechanisms

4.1 Air interface authentication mechanisms

4.1.1 Overview

Authentication is optional, however if it is used it shall be as described in this clause.

The authentication method described is a symmetric secret key type. In this method one secret, the authentication key, shall be shared by each of the authenticating parties, and there should be strictly two parties with knowledge of the secret. Authentication shall be achieved by the parties proving to each other knowledge of the shared secret.

The authenticating parties shall be the authentication centre of the Switching and Management Infrastructure (SwMI) and the Mobile Station (MS). The MS is considered, for the purposes of authentication, to represent the user as defined by the Individual TETRA Subscriber Identity (ITSI). At the air interface the Base Station (BS) is assumed to be trusted by the SwMI and the authentication exchange proves knowledge given to the BS by the authentication centre. This knowledge shall be the session authentication key.

Authentication and provision of keys for use at the air interface shall be linked by the use of a common algorithm set. This algorithm set shall include a means of providing keys for use in group calls. The controlling party in all authentication exchanges shall be the SwMI.

The authentication process describes a 3-pass challenge-response-result protocol.

It is assumed that the intra-system interface linking the BS to the authentication centre is adequately secure.

4.1.2 Authentication of a user

In this subclause, a mechanism is described that shall be used to achieve the authentication of a user of an MS by the SwMI. This shall be done using a challenge response protocol, with a session authentication key derived from an authentication key that shall be shared by the user and the infrastructure. The session authentication key shall be provided by an authentication centre of the home system.

The computation of the session authentication key shall be carried out by an algorithm, TA11. The computation of the response shall be done by another algorithm, TA12, which at the same time shall produce a derived cipher key.

The BS shall generate a random number as a challenge RAND1. The MS shall compute a response, RES1, and the BS shall compute an expected response, XRES1. A derived cipher key shall be generated