SLOVENSKI STANDARD
SIST ETS 300 396-6:1999

01-november-1999

Prizemni snopovni radio (TETRA) - Vseevropski snopovni radijski sistem (TETRA) - Neposredni način zveze (DMO) - 6. del: Varnost

Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security

Ta slovenski standard je istoveten z: ETS 300 396-6 Edition 1

ICS:

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

SIST ETS 300 396-6:1999 en

EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 396-6

April 1998

Source: TETRA

Reference: DE/RES-06007-6

ICS: 33.020

Key words: Direct Mode, security, TETRA

Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: 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
Internet: secretariat@etsi.fr - http://www.etsi.fr - http://www.etsi.org

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

Whilst every care has been taken in the preparation and publication of this document, errors in content, typographical or otherwise, may occur. If you have comments concerning its accuracy, please write to "ETSI Editing and Committee Support Dept." at the address shown on the title page.

Contents

Blank page

Foreword

This European Telecommunication Standard (ETS) has been produced by the Terrestrial Trunked Radio (TETRA) Project 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:	"Direct MS-MS Air Interface- Radio Aspects".
Part 3:	"Direct MS-MS Air Interface- Protocol".
Part 4:	"Repeater Mode Air Interface".
Part 5:	"Gateway Mode Air Interface".
Part 6:	**"Security".**

Transposition dates	
Date of adoption of this ETS:	3 April 1998
Date of latest announcement of this ETS (doa):	31 July 1998
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	31 January 1999
Date of withdrawal of any conflicting National Standard (dow):	31 January 1999

Blank page

1 Scope

This ETS defines the Terrestrial Trunked Radio system (TETRA) Direct Mode of operation. It specifies the basic Air Interface (AI), the interworking between Direct Mode Groups via Repeaters, and interworking with the TETRA trunked system via Gateways. It also specifies the security aspects in TETRA Direct Mode, and the intrinsic services that are supported in addition to the basic bearer and teleservices.

This part describes the security mechanisms in TETRA Direct Mode. It provides mechanisms for confidentiality of control signalling and user speech and data at the AI.

- Clause 4 describes the general condition for which security of calls at the AI can be met. This introduces conditions that all other clauses must follow.

- Clause 5 describes authentication mechanisms for direct mode. The differences between peer-to-peer authentication mechanisms and client-server authentication mechanisms are covered by this clause as are the principles of operation in gateway mode.

- Clause 6 describes the confidentiality mechanisms using encryption on the AI, for circuit mode speech, circuit mode data, packet (short) data and control information. This clause then details the protocol concerning control of encryption at the AI.

- Clause 7 describes the key management mechanism, and includes a description of the OTAR mechanism and protocol.

- Clause 8 describes the enable/disable mechanism and includes a description of the protocol.

- Clause 9 describes the mechanism to be used to support end-to-end encryption using synchronous stream cipher units for U-plane traffic by means of a frame stealing device for synchronization of the units.

- Annex A defines the mapping of protocols in TETRA V+D Security to those of DMO Security for each of OTAR and Enable/Disable.

The use of AI encryption gives confidentiality protection against eavesdropping only. The addition of a synchronized time variant initialization value for the encryption algorithm gives a restrictive degree of replay protection.

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

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

[3] ETS 300 396-1: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Direct Mode; Part 1: General network design".

[4] ETS 300 396-2: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Direct Mode; Part 2: Direct MS-MS Air Interface - Radio Aspects".

[5] ETS 300 392-7: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security"

[6] ETS 300 396-3: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Direct Mode; Part 3: Direct MS-MS Air Interface - Protocol".

[7] ETS 300 396-5: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Speech codec for full-rate traffic channel Part 1: General description of speech functions".

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

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

3 Definitions and abbreviations

3.1 Definitions

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

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

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 (ISO 7498-2 [2]).

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

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

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 Key Stream Generator (KSG) in the transmitting terminal in case synchronization data is not received correctly.

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 Static Cipher Key SCK has been incorrectly recovered in an OTAR exchange.

plain text: The unencrypted source data. The semantic content is available.

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

SCK-set: The collective term for the group of 32 SCK associated with each Individual TETRA Subscriber Identity (ITSI).

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 AI.

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 cipher key that is independent of any other key.

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.

3.2 Abbreviations

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

AC	Authentication Centre
AI	Air Interface
C-PLANE	Control-PLANE
CT	Cipher Text
DLL	Data Link Layer
DM	Direct Mode
DMCC	Direct Mode Call Control
DMO	Direct Mode Operation
EKSG	End-to-end Key Stream Generator
EKSS	End-to-end Key Stream Segment
F	Function
FN	Frame Number
HSC	Half-Slot Condition
HSI	Half-Slot Importance
HSN	Half-Slot Number
HSS	Half-Slot Stolen
HSSE	Half-Slot Stolen by Encryption unit
ITSI	Individual TETRA Subscriber Identity
IV	Initialization Value
K	authentication Key
KH	Key Holder
KS	Session Key
KSG	Key Stream Generator
KSL	Key SeaLer
KSO	Session Key OTAR
KSS	Key Stream Segment
KU	Key User
LLC	Logical Link Control
MAC	Medium Access Control
MF	Manipulation Flag
MNI	Mobile Network Identity
MS	Mobile Station
MSC	Message Sequence Chart
OTAR	Over The Air Rekeying
PDU	Protocol Data Unit

PT	Plain Text
RAND	RANDom challenge
RES	RESponse
RS	Random Seed
RSO	Random Seed for OTARSession Key OTAR
SAP	Service Access Point
SCH	Signalling CHannel
SCH/F	Full SCH
SCH/H	Half SCH
SCH/S	Synchronization SCH
SCK	Static Cipher Key
SCK-VN	SCK Version Number
SCKN	Static Cipher Key Number
SDS	Short Data Service
SDU	Service Data Unit
SHSI	Stolen Half-Slot Identifier
SS	Synchronization Status
SSCK	Sealed Static Cipher Key
STCH	STolen CHannel
SV	Synchronization Value
SwMI	Switching and Management Infrastructure
TA	TETRA Algorithm
TCH	Traffic CHannel
TDMA	Time Division Media Access
TEI	TETRA Equipment Identity
TN	Timeslot Number
TSI	TETRA Subscriber Identity
TVP	Time Variant Parameter
Tx	Transmit
U-PLANE	User-PLANE
V+D	Voice + Data
XRES	eXpected RESponse

4 Operational Security

This clause describes the operational use of security features in TETRA Direct Mode Operation (DMO).

For this clause a call is defined as the group of transmissions and changeovers that are bounded by initial call setup and final call cleardown. Call pre-emption when successful may mark the start of a new call.

NOTE: A DMO call may be considered as a series of unidirectional call transactions with each new call transaction having a new call master (the current transmitter).

A new call master (i.e. call master for the current call transaction) should not be able to change the encryption parameters set at the start of the call. A call shall remain in the same encryption state in all call transactions.

In a standard direct mode call slot 1 of the TDMA structure shall be used by the transmitter for transmission, and slot 3 of the TDMA structure shall be used by the transmitter to send or receive control messages. In frequency efficient operation the other 2 slots of the TDMA structure shall be used in like manner.

4.1 Single-Hop Calls

A DMO call is considered a single-hop call in the following cases:

- MS to individual MS;
- MS to group of MSs.

A single hop call can only be made secure (encrypted) if the following conditions apply:

- Source and Destination MS share SCK;
- Source and Destination MS have common KSG.

Call setup in DMO is a single pass operation with an allowed exception for individual calls to allow a presence check acknowledgement (2 pass call setup). All call parameters are contained in the synchronization bursts which contain two data blocks of 60 bits and 124 bits respectively. The first data block (logical channel SCH/S) shall contain the parameters for encryption. The second data block (logical channel SCH/H) shall contain the addressing data for the call (see ETS 300 396-3 [6], subclause 9.1.1).

4.2 Multi-Hop Calls

DMO calls that pass through a repeater or gateway shall be considered multi-hop calls.

A multi-hop call can only be made secure (encrypted) if one of the following apply (in addition to the conditions for single hop calls):

- the Time Variant Parameter (TVP) used to synchronize the Key Stream Generator (KSG) is unaltered by the transmission;

- intermediate terminations decrypt and re-encrypt the call on each side of the hop.

Calls made through a layer-1 repeater shall not be considered by this ETS. The term repeater when used in later clauses of this ETS shall refer to a layer-2 repeater.

In the case of a call through a gateway to TETRA V+D the DMO call initiator shall be synchronized to the gateway.