SLOVENSKI STANDARD
SIST EN 300 396-6 V1.2.1:2006

01-april-2006

Prizemni snopovni radio (TETRA) ï Neposredni naļ in zveze (DMO) ï 6. del: Varnost

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

Ta slovenski standard je istoveten z: **EN 300 396-6 Version 1.2.1**

ICS:

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

SIST EN 300 396-6 V1.2.1:2006 **en**

ETSI EN 300 396-6 V1.2.1 (2004-05)

European Standard (Telecommunications series)

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

Reference

REN/TETRA-06070

Keywords

air interface, data, DMO, security, speech, TETRA

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, send your comment to:
editor@etsi.org

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 Project Terrestrial Trunked Radio (TETRA).

The present document is part 6 of a multi-part deliverable covering Direct Mode Operation, as identified below:

ETS 300 396-1: "General network design";

EN 300 396-2: "Radio aspects";

ETS 300 396-3: "Mobile Station to Mobile Station (MS-MS) Air Interface (AI) protocol";

EN 300 396-4: "Type 1 repeater air interface";

ETS 300 396-5: "Gateway air interface";

EN 300 396-6: "Security";

EN 300 396-7: "Type 2 repeater air interface";

EN 300 396-8 "Protocol Implementation Conformance Statement (PICS) proforma specification";

EN 300 396-10: "Managed Direct Mode Operation (M-DMO)".

NOTE: Part 8 of this multi-part deliverable is of status "historical" and will not be updated according to this version of the standard.

National transposition dates	
Date of adoption of this EN:	21 May 2004
Date of latest announcement of this EN (doa):	31 August 2004
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	28 February 2005
Date of withdrawal of any conflicting National Standard (dow):	28 February 2005

Introduction

The present document differs from edition 1 of the DMO security specification in the following key areas:

- algorithm specifications have been **moved** to normative annexes:
  - annex A gives the specification of the Key Stream Generator used in providing confidentiality on the air interface; and
  - annex B gives the specification of the Static Cipher Key modification algorithm TB6 that adds variability to the Key Stream Segment output by the Key Stream Generator.
- the enable-disable operations have been **deleted** in favour of operations from a SwMI (TETRA Trunked Operation);
- the re-keying protocol and mechanisms have been **deleted** in favour of operations from a SwMI (TETRA Trunked Operation);
- the end-to-end encryption clause has been **deleted** (and is available in ETSI deliverable EN 302 109 [7]);
- the annexes describing mappings between DMO and TMO security protocols have been **deleted** as the OTAR and ENDIS functions that need to be mapped no longer exist;
- DMO security classes have been defined **replacing** the "Encryption mode element" **and aligning** behaviour to EN 300 392-7 [4]. The description of these classes has been **moved** to clause 4 as this is the most significant aspect of the document;
- a **new** clause describing the interaction of security with the DM call is added which describes both the normal and exceptional behaviour to take on examination of the security elements contained in the synchronization burst;
- "hanging" clauses have been **eliminated** as per the ETSI drafting rules;
- references to V+D have been **replaced** by reference to TMO (Trunked Mode Operation); and
- encryption synchronization has been **promoted** to a full clause.

In addition the "protocol" description identifying the service primitives has been identified as informative (not testable) and has been moved to an informative annex.

1 Scope

The present document 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. It also provided some implicit authentication as a member of a group by knowledge of a shared secret encryption key.

The use of AI encryption gives both confidentiality protection against eavesdropping, and some implicit authentication.

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 and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[1] ETSI EN 300 392-2: "Terrestrial 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] ETSI EN 300 396-2: "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 2: Radio aspects".

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

[5] ETSI ETS 300 396-3: "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 3: Mobile Station to Mobile Station (MS-MS) Air Interface (AI) protocol".

[6] ETSI TS 100 392-15: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 15: TETRA frequency bands, duplex spacings and channel numbering".

[7] ETSI EN 302 109: "Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption".

[8] ETSI ETS 300 396-5: "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 5: Gateway air interface".

[9] ETSI EN 300 396-4: "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 4: Type 1 repeater air interface".

3 Definitions and abbreviations

3.1 Definitions

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

air interface encryption state: status of encryption in a call (on or off)

call transaction: all of the functions associated with a complete unidirectional transmission of information during a call

NOTE: A call is made up of one or more call transactions. In a simplex call these call transactions are sequential. (Source: ETS 300 396-3 [5]).

carrier number: integer, N, used in TETRA to represent the frequency of the RF carrier

NOTE: Source: TS 100 392-15 [6].

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 (ISO 7498-2 [2]).

decipherment: reversal of a corresponding reversible encipherment

NOTE: ISO 7498-2 [2]

Direct Mode Operation (DMO): mode of simplex operation where mobile subscriber radio units may communicate using radio frequencies which may be monitored by, but which are outside the control of, the TETRA TMO network

NOTE: DM operation is performed without intervention of any base station. (Source: ETS 300 396-3 [5]).

DMO-net: number of DMO MSs communicating together and using common cryptographic parameters

encipherment: cryptographic transformation of data to produce cipher text

NOTE: ISO 7498-2 [2]

encryption cipher key: cipher key used as input to the KSG, derived from an address specific cipher key and randomly varied per channel using algorithm TB6

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

explicit authentication: transaction initiated and completed specifically to demonstrate knowledge of a shared secret where the secret is not revealed

implicit authentication: authenticity demonstrated by proof of knowledge of a shared secret where that demonstration is a by-product of another function

key stream: 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

NOTE: The initial state of the KSG is determined by the initialization value.

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

plain text: unencrypted source data.

NOTE: The semantic content is available.

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

SCK-set: collective term for the group of 32 SCKs associated with each Individual TETRA Subscriber Identity

SCK-subset: collection of SCKs from an SCK-set, with SCKNs in numerical sequence, where every SCK in the subset is associated with one or more different GSSIs

NOTE: Multiple SCK subsets have corresponding SCKs associated with the same GSSIs.

Static Cipher Key (SCK): predetermined cipher key that may be used to provide confidentiality in class DM-2-A, DM-2-B and DM-2-C systems with a corresponding algorithm

Synchronization value: 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: encryption method in which a cipher text symbol completely represents the corresponding plain text symbol

NOTE: 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

Trunked Mode Operation (TMO): operations of TETRA specified in EN 300 392-2 [1]

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

ACK	ACKnowledgement
AI	Air Interface
CK	Cypher Key
CN	Carrier Number
DM	Direct Mode
DMAC	Direct Mode Media Access Control
DMC	A layer 2 Service Access Point (DMC-SAP)
DMCC	Direct Mode Call Control
DMO	Direct Mode Operation
ECK	Encryption Cipher Key
EDSI	Encrypted Direct-mode Short Identity
FN	Frame Number
GSSI	Group Short Subscriber Identity
GTSI	Group TETRA Subscriber Identity
KAG	Key Association Group
KSG	Key Stream Generator
KSS	Key Stream Segment
KST	Key Stream Generator
MAC	Medium Access Control
MDE	Message Dependent Elements
MNI	Mobile Network Identity
MS	Mobile Station
OTAR	Over The Air Rekeying
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
REP	Repeater
RF	Radio Frequency
SAP	Service Access Point
SCH	Signalling CHannel
SCH/F	Full SCH
SCH/H	Half SCH
SCH/S	Synchronization SCH
SCK	Static Cipher Key
SCKN	Static Cipher Key Number
SCK-VN	SCK Version Number

SDS	Short Data Service
SDU	Service Data Unit
SSI	Short Subscriber Identity
STCH	STolen CHannel
SwMI	Switching and Management Infrastructure
SYNC	Synchronisation
TCH	Traffic CHannel
TDMA	Time Division Media Access
TMO	Trunked Mode Operation
TN	Timeslot Number
TVP	Time Variant Parameter
U-PLANE	User-PLANE
V+D	Voice + Data
XOR	Exclusive OR

4 DMO security class

4.1 General

TETRA security is defined in terms of class. DMO security offers 4 classes defined in table 1.

NOTE: DMO offers equivalence to TMO security class 1 (no encryption enabled) and to TMO security class 2 (SCK encryption supported).

Table 1: Direct Mode security class

DMO security class	Remark
DM-1	No encryption applied.
DM-2-A	The DM-SDU and any related traffic is AI encrypted. Addresses are not encrypted.
DM-2-B	The destination address (SSI), DM-SDU and any related traffic are AI encrypted.
DM-2-C	In the DMAC-SYNC PDU, the PDU is encrypted from destination address element and onwards except for source address type element, and any related traffic is AI encrypted. In the DMAC-DATA PDU, the PDU is encrypted from the destination address type element and onwards.
NOTE 1: Except in DMAC-DATA PDUs for class DM-2-C the destination and source address type elements are never encrypted. NOTE 2: DM-1 is considered the lowest level of security. NOTE 3: DM-2-A through DM-2-B to DM-2-C provide progressively increased levels of security by encrypting more of the signalling content.	

The security class is identified in DMAC-SYNC PDUs by the AI encryption state element (see table 2).

Table 2: AI encryption state element encoding

Information element	Length	Value	Class
Air Interface encryption state	2	00_2	DM-1
		10_2	DM-2-A
		11_2	DM-2-B
		01_2	DM-2-C

On establishing a call the first master shall establish the security class of the call. The security class should be maintained for the duration of the call.

4.2 DM-2-A

The purpose of security class DM-2-A is to provide confidentiality of user traffic and signalling in applications where it is not necessary to hide the addressing information.

In addition security class DM-2-A allows calls to be made through a repeater where the repeater is not provided with the capability to encrypt or decrypt messages by maintaining the layer 2 (MAC) elements of any signalling in clear.

4.3 DM-2-B

The purpose of security class DM-2-B is to provide confidentiality of user traffic and signalling.

Security class DM-2-B extends the confidentiality applied to signalling over that provided in class DM-2-A to encrypt parts of the MAC header. The encryption allows repeater operation to be made without requiring the repeater to be able to encrypt and decrypt transmissions unless it wishes to check the validity of the destination address. In class DM-2-B because the source address is in clear, a pre-emptor can identify the pre-emption slots and hence the call can be pre-empted even if the pre-emptor does not have the encryption key being used by the call master.

4.4 DM-2-C

The purpose of security class DM-2-C is to provide confidentiality of user traffic and signalling including all identities other than those of repeaters and gateways.

In addition in class DM-2-C the bulk of the MAC header elements are encrypted. Where repeaters are used, the repeater requires the ability to encrypt and decrypt all transmissions. In class DM-2-C calls can only be pre-empted by an MS which has the SCK in use by the call master.

5 DMO call procedures

5.1 General

5.1.1 Security profile

An MS should maintain a security profile for each destination address. The security profile should contain at least the following for each destination address:

- KSG, as identified by its KSG-identifier;
- current SCK, as identified by SCKN, for transmission;
- valid SCKs, as identified by SCKN, for reception;
- the preferred, and minimum, security class to be applied to calls for transmission;
- the minimum security class to be applied to calls for reception; and
- the minimum security class that a master will accept in a pre-emption request.

The preferred security class is the security class to be used for transmission when the MS is acting as a call master. The minimum security class for transmission is the lowest security class that the MS shall use to transmit responses to other signalling.

NOTE 1: Minimum may be the same as preferred.

NOTE 2: A default profile may be maintained in addition to a profile for specific addresses.

NOTE 3: A profile should exist for received individual calls (i.e. for calls where destination address is that of the receiving MS).