SLOVENSKI STANDARD
SIST EN 302 109 V1.1.1:2003

01-december-2003

Prizemni snopovni radio (TETRA) – Varnost – Mehanizem za sinhronizacijo šifriranja zveze konec-konec

Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption

Ta slovenski standard je istoveten z: EN 302 109 Version 1.1.1

ICS:

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

SIST EN 302 109 V1.1.1:2003 **en**

ETSI EN 302 109 V1.1.1 (2003-10)

European Standard (Telecommunications series)

Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption

Reference
DEN/TETRA-06117

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

Copyright Notification

Contents

Intellectual Property Rights 4
Foreword 4
Introduction 4
1 Scope 5
2 References 5
3 Definitions and abbreviations 5
3.1 Definitions 5
3.2 Abbreviations 6
4 End-to-end encryption 7
4.1 Introduction 7
4.2 Voice encryption and decryption mechanism 7
4.2.1 Protection against replay 8
4.3 Data encryption mechanism 8
4.4 Exchange of information between encryption units 9
4.4.1 Synchronization of encryption units 9
4.4.2 Encrypted information between encryption units 10
4.4.3 Transmission 10
4.4.4 Reception 12
4.4.5 Stolen frame format 12
4.5 Location of security components in the functional architecture 13
4.6 End-to-end Key Management 15
Annex A (informative): Bibliography 16
History 17

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).

National transposition dates	
Date of adoption of this EN:	3 October 2003
Date of latest announcement of this EN (doa):	31 January 2004
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	31 July 2004
Date of withdrawal of any conflicting National Standard (dow):	31 July 2004

Introduction

The present document replaces the end-to-end encryption clause in each of EN 300 392-7 and ETS 300 396-6.

1 Scope

The present document defines the Terrestrial Trunked Radio system (TETRA) synchronization operation for end-to-end encryption algorithms that employ streaming ciphers for voice. The method defined applies equally to Direct Mode Operation (as defined in EN 300 396 (see bibliography)) and to Trunked Mode Operation (as defined in EN 300 392 (see bibliography)).

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 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 the present document, the following terms and definitions apply:

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 (ISO 7498-2 [2])

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

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

flywheel: 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): 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

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

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.

time stamp: sequence of symbols that represents the time of day

3.2 Abbreviations

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

AI	Air Interface
CK	Cipher Key
C-plane	Control-plane
CT	Cipher Text
DMD-SAP	Direct Mode D Service Access Point
DMO	Direct Mode Operation
EKSG	End-to-end Key Stream Generator
EKSS	End-to-end Key Stream Segment
F	Function
HSC	Half-Slot Condition
HSI	Half-Slot Importance
HSN	Half-Slot Number
HSS	Half-Slot Stolen
HSSE	Half-Slot Stolen by Encryption unit
IV	Initialization Value
KSG	Key Stream Generator
KSS	Key Stream Segment
L1	Layer 1
L2	Layer 2
L3	Layer 3
MAC	Medium Access Control
MS	Mobile Station
PT	Plain Text
SAP	Service Access Point
SHSI	Stolen Half-Slot Identifier
STCH	Stolen Channel
SV	Synchronization Value
T/DMA-SAP	Trunked or Direct Mode A Service Access Point
T/DMC-SAP	Trunked or Direct Mode C Service Access Point
T/DMD-SAP	Trunked or Direct Mode D Service Access Point
TMD-SAP	Trunked Mode D Service Access Point
Tx	Transmit
U-plane	User-plane
V+D	Voice + Data

4 End-to-end encryption

4.1 Introduction

End-to-end encryption algorithms and key management are outside the scope of the present document. This clause describes a standard mechanism for synchronization of the encryption system that may be employed when using a synchronous stream cipher. The mechanism also permits transmission of encryption related and other signalling information. The mechanism shall apply only to U-plane traffic and U-plane signalling. The method described uses the Stealing Channel, STCH, for synchronization during transmission (see EN 300 392-2 [1], clause 23.8.4).

NOTE: This mechanism does not apply for self-synchronizing ciphers, or for block ciphers.

The following are requirements on the end-to-end encryption mechanism:

- the same mechanisms shall apply in both directions;
- the synchronization processes shall be independent in each direction;
- end-to-end encryption shall be located in the U-plane (above the MAC resident air-interface encryption);
- transport of plain text and cipher text shall maintain the timing and ordering of half-slot pairing (half slots shall be restored in the same order and with the same boundary conditions at each end of the link);
- the encryption mechanisms described in this clause are valid for one call instance.

4.2 Voice encryption and decryption mechanism

Figure 1 shows a functional diagram of the voice encryption and decryption mechanism based on the synchronous stream cipher principle. This demonstrates the symmetry of transmitter and receiver with each side having common encryption units.

It is assumed that the encryption unit shall generate a key stream in a similar way to the AI encryption unit. The encryption unit is then termed the End-to-end Key Stream Generator (EKSG). EKSG shall have two inputs, a cipher key and an initialization value. The initialization value should be a time variant parameter (e.g. a sequence number or a timestamp) that is used to initialize synchronization of the encryption units. The output of EKSG shall be a key stream segment termed EKSS.

Function F_1 shall combine the Plain Text (PT) bit stream and EKSS resulting in an encrypted Cipher Text (CT) bit stream. Function F_1^{-1} shall be the inverse of F_1 and shall combine the bit streams CT and EKSS resulting in the decrypted bit stream PT.

Function F_2 shall replace a half slot of CT with a synchronization frame provided by the "sync control" functional unit.

Function F_3 shall recognize a synchronization frame in the received CT, and shall supply them to "sync detect" functional unit.