SLOVENSKI STANDARD
SIST ETS 300 394-5-2 E1:2003

01-december-2003

Prizemni snopovni radio (TETRA) - Specifikacija za preskušanje skladnosti - 5. del: Varnost - 2. poddel: Specifikacija za preskušanje protokola za varnost v sistemu TETRA

Terrestrial Trunked Radio (TETRA); Conformance testing specification; Part 5: Security; Sub-part 2: Protocol testing specification for TETRA security

Ta slovenski standard je istoveten z: ETS 300 394-5-2 Edition 1

ICS:

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

SIST ETS 300 394-5-2 E1:2003 **en**

EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 394-5-2

July 1999

Source: TETRA

Reference: DE/TETRA-06009-5-2

ICS: 33.020

Key words: TETRA, security, voice, data, V+D, testing, protocol

Terrestrial Trunked Radio (TETRA); Conformance testing specification; Part 5: Security; Sub-part 2: Protocol testing specification for TETRA 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.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 Standards Making Support Dept." at the address shown on the title page.

Contents

Foreword 7

1 Scope 9

2 Normative references 9

3 Definitions and abbreviations 10
3.1 TETRA definitions 10
3.2 TETRA abbreviations 10
3.3 ISO 9646 abbreviations 10

4 Test Suite Structure (TSS) 11
4.1 Security TSS overview 11
4.2 Security test groups 12
4.2.1 V+D Security test group 12
4.2.2 DM Security test group 12
4.3 Test group description 13

5 Introduction to Test Purposes (TPs) 13
5.1 TP definition conventions 13
5.2 TP naming conventions 14

6 Test Purposes for V+D 14
6.1 Steps 14
6.1.1 Check encryption state 15
6.1.2 Check enable state 15
6.1.3 Check permanent disabled 15
6.1.4 Check temporary disable 15
6.2 Authentication 15
6.2.1 Authentication initiated by the SwMI 15
6.2.1.1 SwMI authenticates MS 16
6.2.1.2 Authentication initiated by SwMI and made mutual by MS 16
6.2.2 Authentication procedures initiated by the MS 17
6.2.2.1 MS authenticates SwMI 17
6.2.2.2 Authentication initiated by MS and made mutual by SwMI 18
6.2.3 Authentication procedures during registration 18
6.2.3.1 SwMI authenticates MS during registration 18
6.2.3.2 MS authenticates SwMI during registration 19
6.2.3.3 Authentication initiated by MS during registration made mutual by SwMI 20
6.2.3.4 SwMI authentication initiated during registration and made mutual by the MS 20
6.2.3.5 Authentication during registration with CCK delivery 21
6.2.3.5.1 SwMI authenticates MS during registration and delivers CCK 21
6.2.3.5.2 MS authenticates SwMI during registration and request CCK 22
6.2.3.5.3 Authentication initiated by MS during registration including a CCK request and made mutual by SwMI 22
6.2.3.5.4 SwMI authentication initiated during registration and made mutual by the MS with CCK exchange 23
6.2.3.6 Authentication procedures during registration with TEI exchange 24

6.2.3.6.1 SwMI authenticates MS during registration and includes a TEI request 24
6.2.3.6.2 MS authenticates SwMI during registration and the SwMI request TEI .24
6.2.3.6.3 Authentication initiated by MS during registration including a TEI exchange and made mutual by SwMI 25
6.2.3.6.4 SwMI authentication initiated during registration and made mutual by the MS with TEI exchange 26
6.2.3.7 Authentication procedures during registration with TEI and CCK exchange....26
6.2.3.7.1 SwMI authenticates MS during registration, delivers CCK and receives TEI 27
6.2.3.7.2 MS authenticates SwMI during registration and delivers TEI and request CCK 27
6.2.3.7.3 Authentication initiated by MS during registration including TEI, CCK exchange and made mutual by SwMI...28
6.2.3.7.4 SwMI authentication initiated during registration and made mutual by the MS with TEI and CCK exchange 29
6.2.4 Unsuccessful authentication procedures 29
6.2.4.1 Unsuccessful authentication initiated by MS 30
6.2.4.2 Unsuccessful MS authentication during mutual authentication initiated by the SwMI 30
6.2.4.3 Unsuccessful SwMI authentication during mutual authentication initiated by the SwMI 31
6.2.4.4 Unsuccessful mutual authentication initiated by MS....32
6.3 TEI delivery during registration without authentication....32
6.3.1 TEI delivery during registration without authentication....32
6.4 OTAR....33
6.4.1 CCK delivery functions....33
6.4.1.1 SwMI-initiated CCK provision 33
6.4.1.2 MS-initiated CCK provision....35
6.4.1.3 MS-initiated CCK provision in a U-PREPARE PDU 35
6.4.1.3.1 MS roams into a new cell in the same LA and the same registration area....35
6.4.1.3.2 MS roams into a new cell in a different LA and the same registration area....36
6.4.1.3.3 MS roams into a new cell in a different LA and different registration area 36
6.4.1.4 SwMI provides an incorrect CCK to MS 37
6.4.2 OTAR protocol functions SCK....37
6.4.2.1 MS initiates provision of SCK 38
6.4.2.2 SwMI initiates SCK to MS....38
6.4.2.3 SwMI provides an incorrect SCK....39
6.4.3 OTAR protocol functions GCK 40
6.4.3.1 MS requests provision of GCK 40
6.4.3.2 SwMI provides GCK to MS....41
6.4.3.3 SwMI unable to provide GCK requested by MS 41
6.4.3.4 SwMI provides an incorrect GCK to MS 42
6.5 Enable and Disable....43
6.5.1 Disable procedures 43
6.5.1.1 Disable with mutual authentication 43
6.5.1.2 Disable without authentication....46
6.5.1.3 Disable failure....47
6.5.2 Enable procedures 51
6.5.2.1 Enable with mutual authentication....51
6.5.2.2 Enable without authentication....52

6.5.2.3 Enable failure 53
6.6 Mobility management for Air Interface Encryption 54
6.6.1 MS registration at initial class 1 cell selection 54
6.6.2 MS registration at initial class 2 or 3 cell selection 55

7 Test purposes for DMO 55
7.1 Layer 2 55
7.2 Layer 3 56
7.2.1 OTAR 56
7.2.1.1 IUT requests SCK 56
7.2.1.2 IUT provides SCK 57
7.2.1.2.1 MS as a KH provides SCK to the KU 57
7.2.1.2.2 IUT as a KH requests SCK to KG 58
7.2.1.3 KH distributing SCK unsolicited 58
7.2.1.4 Error scenario with SDS time-out from KH 59
7.2.1.5 KG provides an incorrect SCKN 59
7.2.2 Enable and disable 60
7.2.2.1 Disable 60
7.2.2.1.1 MS supports the target role 60
7.2.2.1.2 MS supports the manager role 62
7.2.2.2 Enable 64
7.2.2.2.1 MS support the target role 64
7.2.2.2.2 MS support the manager role 65
7.2.2.3 TEI delivery 66
7.2.2.4 Authentication failure in ENDIS exchange 67

History 68

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).

Every ETS prepared by ETSI is a voluntary standard. This ETS contains text concerning conformance testing of the equipment to which it relates. This text should be considered only as guidance and does not make this ETS mandatory.

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

Part 1:	"Radio";
Part 2:	"Protocol testing specification for Voice plus Data (V+D)";
Part 4:	"Protocol testing specification for Direct Mode Operation (DMO)";
Part 5:	**"Security".**

Transposition dates	
Date of adoption of this ETS:	25 June 1999
Date of latest announcement of this ETS (doa):	30 September 1999
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	31 March 2000
Date of withdrawal of any conflicting National Standard (dow):	31 March 2000

Blank page

1 Scope

This ETS contains the Test Suite Structure (TSS) and Test Purposes (TPs) to test the TETRA security protocols for Voice + Data (V+D) and Direct Mode (DM).

The TPs presented in this ETS are applicable to TETRA terminals supporting security as specified in ETS 300 392-2 [1], ETS 300 392-7 [2] and ETS 300 396-6 [3].

The objective of this test specification is to provide a basis for approval tests for TETRA equipment giving a high probability of air interface inter-operability between different manufacturer's TETRA equipment.

The ISO standard for the methodology of conformance testing, ISO/IEC 9646-1 [5] and ISO/IEC 9646-2 [6], as well as the ETSI methodology for conformance testing, ETS 300 406 [4], are used as the basis for the test methodology.

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: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".

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

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

[4] ETS 300 406: "Methods for Testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

[5] ISO/IEC 9646-1 (1994): "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 1: General concepts". (See also CCITT Recommendation X.290 (1991))

[6] ISO/IEC 9646-2 (1991): "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 2: Abstract test suite specification". (See also CCITT Recommendation X.291 (1991))

[7] ETS 300 394-5-1: "Terrestrial Trunked Radio (TETRA); Conformance testing specification; Part 5: Security; Sub-part 1: Protocol Implementation Conformance Statement (PICS) proforma specification".

[8] ETS 300 394-5-3: "Terrestrial Trunked Radio (TETRA); Conformance testing specification; Part 5: Security; Sub-part 3: Abstract Test Suite (ATS)".

3 Definitions and abbreviations

3.1 TETRA definitions

For the purposes of this ETS, the definitions given in ETS 300 392-7 [2] and ETS 300 396-6 [3] apply.

3.2 TETRA abbreviations

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

CCK	Common Cipher Key
DM	Direct Mode
DMO	Direct Mode Operation
ITSI	Individual TETRA Subscriber Identity
GCK	Group Cipher Key
KG	Key Generator
KH	Key Holder
KU	Key User
LA	Location Area
MAC	Medium Access Control
MM	Mobility Management
MS	Mobile Station
MSC	Message Sequence Chart
SCK	Static Cipher Key
SDS	Short Data Services sub entity within CMCE
SDU	Service Data Unit
SwMI	Switching and Management Infrastructure
V+D	Voice + Data

3.3 ISO 9646 abbreviations

For the purposes of this ETS, the following ISO 9646-1 [5] abbreviations apply:

ICS	Implementation Conformance Statement
IUT	Implementation Under Test
IXIT	Implementation eXtra Information for Testing
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PIXIT	Protocol Implementation eXtra Information for Testing
TP	Test Purpose
TSS	Test Suite Structure

4 Test Suite Structure (TSS)

4.1 Security TSS overview

The two security test suite, as illustrated in figure 1, are structured as a tree with a first level defined representing the V+D or DM whole test suite for TETRA security protocols.

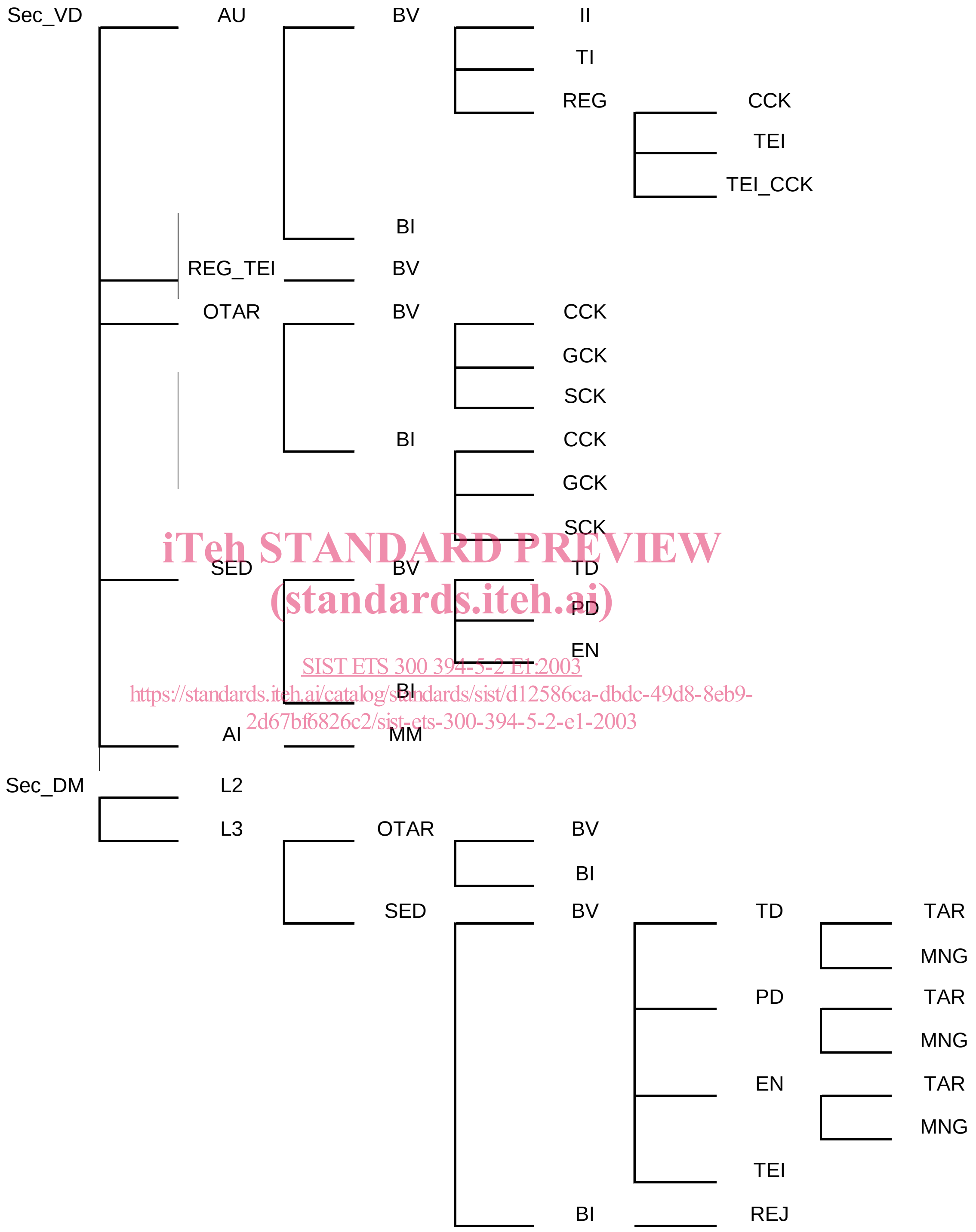

Figure 1: Security TSS

4.2 Security test groups

4.2.1 V+D Security test group

The V+D test groups are organized in several levels. The first level separates protocol test into the different functional capabilities: Authentication (AU), OTAR, Secure Enable/disable (SED) and Air Interface encryption (AI). The second level generally separates protocol test into two functional test groups according to the type of testing: Valid Behaviour (BV), and Invalid Behaviour (BI). The purpose of these test groups is explained in subclause 4.4.

The following list defines the Sec_VD layer test group names and identifiers:

= > to review

- Voice + Data (Sec_VD):

    - Authentication (AU):
        - Valid Behaviour tests (BV):
            - SwMI initiated (II);
            - Terminal initiated (TI);
            - Registration (REG)
                - CCK
                - TEI (TEI)
                - TEI_CCK
        - Invalid Behaviour tests (BI);
    - ■ Registration with TEI (REG_TEI)
        - Valid Behaviour tests (BV):
    - Over The Air Rekeying (OTAR):
        - Valid Behaviour tests (BV):
            - Common Cipher Key (CCK);
            - Group Cipher Key (GCK);
            - Static Cipher Key (SCK);
        - Invalid Behaviour tests (BI):
            - Common Cipher Key (CCK);
            - Group Cipher Key (GCK);
            - Static Cipher Key (SCK);
    - Secure Enable/Disable (SED):
        - Valid Behaviour tests (BV):
            - Temporary disable (TD);
            - Permanent disable (PD);
            - Enable (EN);
        - Invalid Behaviour tests (BI);
    - Air Interface encryption (AI)
    - Mobility management (MM)

4.2.2 DM Security test group

The DM test groups are organized in several levels. The first level separates protocol test into the layer 2 and layer 3 configuration. The second level separates the different functional capabilities: OTAR and Secure Enable/disable (SED). The third level generally separates protocol test into two functional test groups according to the type of testing: Valid Behaviour (BV), and Invalid Behaviour (BI). The purpose of these test groups is explained in subclause 4.4.

The following list defines the S layer test group names and identifiers:

- DM (Sec_DM):
  - Layer 2 (L2):

  - Layer 3 (L3):

    - Over The Air Rekeying (OTAR):
      - Valid Behaviour tests (BV);
      - Invalid Behaviour tests (BI);
    - Secure Enable/Disable (SED):
      - Valid Behaviour tests (BV):
        - Temporary disable (TD):
        - Target role (TAR);
        - Manager role (MNG);
        - Permanent disable (PD):
          - Target role (TAR);
          - Manager role (MNG);
        - Enable (EN):
          - Target role (TAR);
          - Manager role (MNG);
        - TEI delivery (TEI);
        - ENDIS reject (REJ);
      - Invalid Behaviour tests (BI).

4.3 Test group description

The Valid Behaviour (BV) group tests an IUT in response to valid behaviour of the test system. "Valid" means that a test event is syntactically and contextually correct. All test cases in the valid behaviour group are intended to verify as thoroughly as possible the various functions of the protocol.

The Invalid Behaviour (BI) group is intended to verify that the IUT is able to react properly in case an invalid Protocol Data Unit (PDU) occurring. Invalid PDU here means syntactically or semantically invalid test events generated by the test system. A syntactically or semantically invalid test event regardless of the current state is not allowed. Inopportune test cases are also included in this test group. These are intended to verify that the IUT is able to react properly in case an inopportune test event occurs. Such an event is syntactically correct, but occurs when it is not allowed.

5 Introduction to Test Purposes (TPs)

Each TP is defined with the following assumptions:

- the Implementation Under Test (IUT) is a TETRA MS;

- for V+D tests, the test system is a simulation of the TETRA SwMI;

- for DM tests the test system is a simulation of a DM-MS;

- connection to the IUT is by either a test connector or by an RF connection.

The TPs are defined in clause 6 for TETRA V+D security and in clause 7 for DM.

5.1 TP definition conventions

The TPs are defined following particular rules as shown in table 1.