SLOVENSKI STANDARD
SIST ETS 300 812 E1:2003

01-december-2003

Prizemni snopovni radio (TETRA) - Varnostni vidiki - Vmesnik med naroļ niġko identifikacijsko kartico in mobilno opremo (SIM-ME)

Terrestrial Trunked Radio (TETRA); Security aspects; Subscriber Identity Module to Mobile Equipment (SIM - ME) interface

Ta slovenski standard je istoveten z: ETS 300 812 Edition 1

ICS:

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

SIST ETS 300 812 E1:2003 **en**

EUROPEAN TELECOMMUNICATION STANDARD

ETS 300 812

November 1998

Source: TETRA

Reference: DE/TETRA-07017

ICS: 33.020

Key words: Card, security, TETRA

Terrestrial Trunked Radio (TETRA); Security aspects; Subscriber Identity Module to Mobile Equipment (SIM - ME) interface

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

Content

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).

Transposition dates	
Date of adoption of this ETS:	27 November 1998
Date of latest announcement of this ETS (doa):	28 February 1999
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	31 August 1999
Date of withdrawal of any conflicting National Standard (dow):	31 August 1999

Blank page

1 Scope

This ETS defines the interface between the Subscriber Identity Module (SIM) and the Mobile Equipment (ME) for use during the network operation phase of TETRA as well as those aspects of the internal organization of the SIM which are related to the network operation phase. This is to ensure interoperability between a SIM and an ME independently of the respective manufacturers and operators. The concept of a split of the MS into these elements as well as the distinction between the TETRA network operation phase, which is also called TETRA operations, and the administrative management phase is described in the User Requirement Specification ETR 295 [9].

This ETS defines:

- the requirements for the physical characteristics of the SIM, the electrical signals and the transmission protocols;
- the model which shall be used as a basis for the design of the logical structure of the SIM;
- the security features;
- the interface functions;
- the commands;
- the contents of the files required for the TETRA application;
- the application protocol.

This ETS does not specify any aspects related to the administrative management phase. Any internal technical realization of either the SIM or the ME are only specified where these reflect over the interface. This ETS does not specify any of the security algorithms which may be used.

The physical SIM described in this ETS is a removable integrated Circuit (IC) card. The SIM is an optional device within TETRA MSs. This ETS does not preclude the implementation of fully functional MSs without a SIM. All references to mobile equipment in this ETS are to be taken to mean mobile equipment which have been designed to operate with a SIM.

This ETS deals with all aspects of trunked mode MS operation. For direct mode MS operation key user operation is supported by the SIM but not key holder or key generator operation. Furthermore, storage of information for direct mode MS operation in repeater and gateway mode are supported, but any extra storage required in the direct mode repeater or direct mode gateway terminals themselves is not supported.

2 Normative references

This ETS incorporates, by dated or 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] ISO 7810 (1985): "Identification cards - Physical characteristics".

[2] ISO 7811-1 (1995): "Identification cards - Recording technique - Part 1: Embossing".

[3] ISO 7811-3 (1995): "Identification cards - Recording technique - Part 3: Location of embossed characters on ID-1 cards".

[4] ISO/IEC 7816-1 (1987): "Identification cards - Integrated circuit(s) cards with contacts, Part 1: Physical characteristics".

[5] ISO/ISO 7816-2 (1988): "Information technology - Identification cards - Integrated circuit(s) cards with contacts, Part 2: Dimensions and location of the contacts".

[6] ISO/IEC 7816-3 (1997): "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[7] ISO/IEC 7816-4 (1995): "Information technology - Identification cards - Integrated circuit(s) cards with contacts, Part 4: Interindustry commands for interchange".

[8] ENV 1375-1: "Identification card systems - Intersector integrated circuit(s) card additional formats - Part 1: ID-000 card size and physical characteristics".

[9] ETR 295: "User requirements for Subscriber Identity Module (SIM)".

[10] ETS 300 392-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General Network Design".

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

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

[13] 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".

[14] ETS 300 608 (1996): "Digital cellular telecommunications system (Phase 2); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (GSM 11.11)".

[15] ETS 300 641 (1996): "Digital cellular telecommunications system (Phase 2); Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (GSM 11.12)".

[16] ISO/IEC 7816-5 (1994): "Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".

[17] ETS 300 628 (1994): "European digital cellular telecommunications system (Phase 2); Alphabets and language-specific information (GSM 3.38)".

[18] CCITT Recommendation T.50: "International Reference Alphabet (IRA) (Formerly International Alphabet No. 5 or IA5) – Information technology – 7-bit coded character set for information interchange)".

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

[20] ETS 300 392-12-22: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 12: Supplementary services stage 3; Sub-part 22: Dynamic Group Number Assignment (DGNA)".

[21] CCITT Recommendation E.118: "The international telecommunication charge card".

[22] ISO 8859-1 (1987): "Information processing 8 bit-single byte coded graphic character sets - Part 1: Latin alphabet No. 1".

[23] ETS 300 394-2 (1997): "Terrestrial Trunked Radio (TETRA); Conformance testing specification; Part 2: Protocol testing specification for Voice plus Data (V+D)".

3 Definitions, abbreviations and symbols

3.1 Definitions

For the purposes of this ETS, the following definitions apply. For further information and definitions refer to ETS 300 392-1 [10].

access conditions: A set of security attributes associated with access to an Elementary File (EF):

ADM (administrative):

indicates an access condition defined by the card issuer. Before issue of the card ADM serves as a placeholder for an access condition to be defined by the card issuer. Any access condition may be assigned. The assigned access condition is used during the usage phase of the SIM.

AUTI (authorized immediate):

defines access conditions to an EF under which access shall is only possible immediately following successful authentication of the Switching and Management Infrastructure (SwMI).

CHVn (card holder verification):

defines the access condition to an EF which requires verification of the user identity (n = 1 or n = 2).

NEV (never):

access to the EF is never allowed across the SIM-ME interface.

RAU (reserved for administrative use):

defines access conditions to an EF which is restricted to the administrative phase of the SIM.

administrative phase: That part of the card life between the manufacturing phase and the usage phase.

application: An application consists of a set of security mechanisms, files, data and protocols (excluding transmission protocols).

application protocol: The set of procedures required by the application which are located and used in the Integrated Circuit (IC) card and outside the IC card (external application).

card holder verification: Authentication of the user to the SIM card.

card session: A link between the card and the external world starting with the Answer To Reset (ATR) and ending with a subsequent reset or a deactivation of the card.

current directory: The latest Master File (MF) or Dedicated File (DF) selected.

current Elementary File (EF): The latest EF selected.

current file: The latest MF, DF, or EF selected.