SLOVENSKI STANDARD
SIST EN 300 812-3 V2.2.1:2006

01-april-2006

Prizemni snopovni radio (TETRA) - Vmesnik med naroį niġko identifikacijsko kartico in mobilno opremo (SIM-ME) - 3. del: Integrirano vezje (IC) - Fiziį ne, logiį ne in TSIM aplikacijske karakteristike

Terrestrial Trunked Radio (TETRA); Subscriber Identity Module to Mobile Equipment (SIM-ME) interface; Part 3: Integrated Circuit (IC); Physical, logical and TSIM application characteristics

Ta slovenski standard je istoveten z: EN 300 812-3 Version 2.2.1

ICS:

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

SIST EN 300 812-3 V2.2.1:2006 en

ETSI EN 300 812-3 V2.2.1 (2004-02)

European Standard (Telecommunications series)

Terrestrial Trunked Radio (TETRA); Subscriber Identity Module to Mobile Equipment (SIM-ME) interface; Part 3: Integrated Circuit (IC); Physical, logical and TSIM application characteristics

Reference

REN/TETRA-03102

Keywords

card, security, SIM, 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

Content

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).

It was originally published as EN 300 812 (V2.1.1) and then converted into a sub-part EN 300 812-3 to support technology defined in the present document. The other parts of this series are currently published in TS and ES formats:

The present document is part 3 of a multi-part deliverable covering the Subscriber Identity Module to Mobile Equipment (SIM-ME) interface, as identified below:

ES 200 812-1: "Universal Integrated Circuit Card (UICC); Physical and logical characteristics";

ES 200 812-2: "Universal Integrated Circuit Card (UICC); Characteristics of the TSIM application";

EN 200 812-3: "Integrated Circuit (IC); Physical, logical and TSIM application characteristics".

NOTE: Part 3 was originally published as EN 300 812 and defines different technology than part 1 and part 2.

National transposition dates	
Date of adoption of this EN:	20 February 2004
Date of latest announcement of this EN (doa):	31 May 2004
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	30 November 2004
Date of withdrawal of any conflicting National Standard (dow):	30 November 2004

1 Scope

The present document 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 a 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 [6].

The present document 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; This edition of the standard covers the security mechanisms for ITSI based services including authentication and OTAR for keys addressed to an ITSI;
- the interface functions;
- the commands;
- the contents of the files required for the TETRA application;
- the application protocol.

The present document 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. The present document does not specify any of the security algorithms which may be used.

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

The present document 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 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 300 392-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".

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

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

[4] ETSI 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)".

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

[6] ETSI ETR 295: "Terrestrial Trunked Radio (TETRA); User requirements for Subscriber Identity Module (SIM)".

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

[8] Void.

[9] ETSI TS 100 977: "Digital cellular telecommunications system (Phase 2+) (GSM); Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (GSM 11.11)".

[10] ETSI TS 100 900: "Digital cellular telecommunications system (Phase 2+) (GSM); Alphabets and language-specific information (GSM 03.38 version 7.2.0 Release 1998)".

[11] ETSI TS 100 906: "Digital cellular telecommunications system (Phase 2+) (GSM); Mobile Stations (MS) features (GSM 02.07 version 7.1.0 Release1998)".

[12] ETSI TS 100 907: "Digital cellular telecommunications system (Phase 2+); Man-machine Interface (MMI) of the Mobile Station (MS) (3GPP TS 02.30 version 7.1.1 Release 1998)".

[13] ETSI TS 100 927: "Digital cellular telecommunications system (Phase 2+); Numbering, Addressing and Identification (3GPP TS 03.03 version 7.7.0 Release 1998)".

[14] GTS GSM 04.08: "Digital cellular telecommunications system (Phase 2+) (GSM); Mobile radio; Layer 3 specification (GSM 04.08)".

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

[16] ISO/IEC 7810: "Identification cards - Physical characteristics".

[17] ISO/IEC 7811-1: "Identification cards - Recording technique - Part 1: Embossing".

[18] Void.

[19] ISO/IEC 7816-1 (1998): "Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics".

[20] ISO/IEC 7816-2 (1999): "Information technology - Identification cards - Integrated circuit(s) cards with contacts, Part 2: Dimensions and location of the contacts".

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

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

[23] ISO 639 (all parts): "Code for the representation of names of languages".

[24] ISO/IEC 8859-1 (1998): "Information technology - 8 bit-single byte coded graphic character sets - Part 1: Latin alphabet No. 1".

[25] CEN EN 1375: "Identification card system - Intersector integrated circuit(s) card additional formats - ID-000 card size and physical characteristics".

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

[27] ITU-T Recommendation E.118: "The international telecommunication charge card".

[28] ITU-T Recommendation E.164: "The international public telecommunication numbering plan".

[29] ETSI ES 200 812-2: "Terrestrial Trunked Radio (TETRA); Subscriber Identity Module to Mobile Equipment (TSIM-ME) interface; Part 2: Universal Integrated Circuit Card (UICC); Characteristics of the TSIM application".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in EN 300 392-1 [1] and the following apply:

access conditions: 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.

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

application: set of security mechanisms, files, data and protocols (excluding transmission protocols)

application protocol: 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: 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: latest Master File (MF) or Dedicated File (DF) selected

current Elementary File (EF): latest EF selected

current file: latest MF, DF, or EF selected

Dedicated File (DF): file containing access conditions and, optionally, EFs or other DFs

directory: general term for MF and DF

Elementary File (EF): file containing access conditions and data and no other files

file: directory or an organized set of bytes or records in the SIM

file identifier: 2 bytes which address a file in the SIM

key generator: secure system entity authorized to generate Static Cipher Keys (SCKs) for Direct Mode Operation (DMO)

key holder: secure system entity authorized to distribute SCKs for DMO

key user: standard Direct Mode (DM) terminal which uses SCKs provided by an authorized key holder

ID-1 SIM: SIM having the format of an ID-1 card (see ISO/IEC 7816-1 [19])

input: signifies data input to the SIM functions (defined in clause 8):

Input from SIM	input from the SIM internal memory;
Input from EF	internal input from an EF on the SIM;
Input from ME	data contained in a command APDU passed across the SIM-ME interface.

Master File (MF): unique mandatory DF representing the root

Mobile equipment (ME): part of the MS which interfaces to the SIM card

Mobile Station (MS): entirety of the equipment needed to communicate with the infrastructure (in trunked mode of operation) or direct with another MS (in direct mode of operation)

output: signifies data output from the SIM functions (defined in clause 8):

Output to SIM	data shall be stored on the SIM in non-permanent memory for the duration of the TETRA session;
Output to EF	internal updating of an EF on the SIM;
Output to ME	data contained in a response APDU passed across the SIM-ME interface.

padding: one or more bits appended to a message in order to cause the message to contain the required number of bits or bytes

personalization: addition of subscriber and end user data to the appropriate EFs in the SIM during the administrative phase of a card's life cycle

pre-personalization: assignment of EF values at the manufacturing phase of a card's life cycle

plug-in SIM: second format of SIM (specified in clause 4)

record: string of bytes within an EF handled as a single entity (see clause 6)

record number: number which identifies a record within an EF

record pointer: pointer which addresses one record in an EF

Subscriber Identity Module (SIM) or SIM card: integrated circuit card containing network related subscriber information

T = 0: half-duplex asynchronous character based transmission protocol. As defined in ISO/IEC 7816-3 [21]

T = 1: half-duplex asynchronous block based transmission protocol. The protocol may be initiated after ATR. As defined in ISO/IEC 7816-3 [21]

TETRA application: set of security mechanisms, files, data and protocols required by TETRA

TETRA session: part of the card session dedicated to the TETRA operation

TETRA SIM: subscriber identity module used in a TETRA MS

usage phase: part of the card life, after the administrative phase, when the card is being used for operational purposes

5 V technology SIM: SIM operating at 5 V ±10 %

3 V technology SIM: SIM operating at 3 V ±10 % and 5 V ±10 %

3 V technology ME: ME operating the SIM - ME interface at 3 V ±10 % according to ETS 300 641 [15] and 5 V ±10 % according to TS 100 977 [9]

3 V only ME: ME only operating the SIM - ME interface at 3 V ±10 % according to ETS 300 641 [15]

3.2 Symbols

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

"0" to "9" and "A" to "F"	The sixteen hexadecimal digits
Vcc	Supply voltage
Vpp	Programming voltage

3.3 Abbreviations

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

ADM	ADMinistrative (see definitions)
ADN	Abbreviated Dialling Number
ALW	ALWays
APDU	Application Protocol Data Unit
APN	Access Point Name
ASSI	Alias Short Subscriber Identity
ATR	Answer To Reset
AUTI	AUThorized Immediate (see definitions)
BCD	Binary Coded Decimal
CCK	Common Cipher Key
CCK-id	CCK identifier
CHV	Card Holder Verification (see definitions)
CLA	CLAss
CLK	CLocK
DCK	Derived Cipher Key
DCK1	Part 1 of the DCK
DCK2	Part 2 of the DCK
DF	Dedicated File
DGNA	Dynamic Group Number Assignment
DM	Direct Mode
DMO	Direct Mode Operation
DTMF	Dual Tone Multiple Frequency
EF	Elementary File
FDN	Fixed Dialling Number
FSSN	Fleet Specific Short Number
GCK	Group Cipher Key
GCKN	Group Cipher Key Number
GCK-VN	GCK Version Number
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GSSI	Group Short Subscriber Identity
GTSI	Group Tetra Subscriber Identity
I/O	Input/Output
IC	Integrated Circuit
ID	IDentifier
INS	INStruction code
IP	Internet Protocol
ISSI	Individual Short Subscriber Identity
ITSI	Individual TETRA Subscriber Identity
K	individual subscriber authentication Key
KE	Enhanced security Key
KSO	Session Key for Over the air re-keying