SLOVENSKI STANDARD
SIST EN 302 409 V7.0.3:2003

01-december-2003

Digitalni celiļ ni telekomunikacijski sistem (faza 2+) ï Specifikacija naroļ niġke identifikacijske kartice za fiksni del in mobilno postajo v sistemu brezvrviļ ne telefonije (GSM 11.19, razliļ ica 7.0.3, izdaja 1998)

Digital cellular telecommunications system (Phase 2+) (GSM); Specification of the Cordless Telephony System Subscriber Identity Module for both Fixed Part and Mobile Station (GSM 11.19 version 7.0.3 Release 1998)

Ta slovenski standard je istoveten z: **EN 302 409 Version 7.0.3**

ICS:

33.070.50	Globalni sistem za mobilno telekomunikacijo (GSM)	Global System for Mobile Communication (GSM)

SIST EN 302 409 V7.0.3:2003 **en**

ETSI EN 302 409 V7.0.3 (2000-08)

European Standard (Telecommunications series)

Digital cellular telecommunications system (Phase 2+); Specification of the Cordless Telephony System Subscriber Identity Module for both Fixed Part and Mobile Station (GSM 11.19 version 7.0.3 Release 1998)

GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS

Reference
DEN/SMG-091119Q7

Keywords
Digital cellular telecommunications system,
Global System for Mobile communications
(GSM), GSM Cordless Telephony System (CTS)

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://www.etsi.org/tb/status/

If you find errors in the present document, send your comment to:
editor@etsi.fr

Copyright Notification

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://www.etsi.org/ipr).

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 Technical Committee Special Mobile Group (SMG).

The present document was submitted to Public Enquiry with the ETSI number 301 409. For Vote the number was changed to 302 409 because the number 301 409 is reserved and was allocated accidentally.

The present document defines the interface between the Fixed Part Subscriber Identity Module (FP-SIM) and the Cordless Telephony System Fixed Part Equipment (CTS-FPE) within the digital cellular telecommunications system.

The contents of the present document are subject to continuing work within SMG and may change following formal SMG approval. Should SMG modify the contents of the present document it will then be republished by ETSI with an identifying change of release date and an increase in version number as follows:

Version 7.x.y

where:

7 indicates GSM Release 1998 of Phase 2+

x the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

y the third digit is incremented when editorial only changes have been incorporated in the specification..

National transposition dates	
Date of adoption of this EN:	21 July 2000
Date of latest announcement of this EN (doa):	31 October 2000
Date of latest publication of new National Standard or endorsement of this EN (dop/e):	30 April 2001
Date of withdrawal of any conflicting National Standard (dow):	30 April 2001

1 Scope

The present document defines the aspects of the internal organization of the FP-SIM which are related to the CTS initialization and CTS enrolment operation phase of CTS as well as the files contained in the SIM for dedicated CTS operation. This is to ensure interoperability between a FP-SIM and a CTS-FPE independently of the respective manufacturers and operators.

The present document defines:

- the contents of the files required for the CTS application*;*
- the application protocol.

All information regarding the interface between the Fixed Part Subscriber Identity Module (FP-SIM) and the Cordless Telephony System Fixed Part Equipment (CTS-FPE) mentioned below are fully compliant with the TS-GSM11.11 [12] unless otherwise stated in the present document.

- the requirements for the physical characteristics of the FP-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 FP-SIM*;*
- the security features*;*
- the interface functions*;*
- the commands.

For more details regarding CTS, refer to specifications GSM 02.56 [3]and GSM 03.56 [6].

The present document does not specify any aspects related to the administrative management phase. Any internal technical reallocation of either the FP-SIM or the CTS-FPE are only specified where these reflect over the interface. It does not specify any of the security algorithms which may be used.

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, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.
- For this Release 1998 document, references to GSM documents are for Release 1998 versions (version 7.x.y).

[1] GSM 01.02: "Digital cellular telecommunications system (Phase 2+); General description of a GSM Public Land Mobile Network (PLMN)".

[2] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms ".

[3] GSM 02.56: "Digital cellular telecommunications system (Phase 2+); GSM Cordless Telephone System (CTS) Phase 1; Service Description; Stage 1 ".

[4] GSM 03.03: " Digital cellular telecommunications system (Phase 2+); Numbering, addressing and identification ".

[5] GSM 03.20: " Digital cellular telecommunications system (Phase 2+); GSM Cordless Telephony System (CTS), (Phase 1) Security related network functions; Stage 2".

[6] GSM 03.56: "Digital cellular telecommunications system (Phase 2+); GSM Cordless Telephone System (CTS), Phase 1; CTS Architecture Description; Stage 2 ".

[7] GSM 04.08: "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification".

[8] GSM 04.56: "Digital cellular telecommunications system (Phase 2+); GSM Cordless Telephone System (CTS) Phase 1; CTS radio interface layer 3 specification"

[9] GSM 05.05: "Digital cellular telecommunications system (Phase 2+); Radio Transmission and Reception".

[10] GSM 05.08: "Digital cellular telecommunications system (Phase 2+); Radio subsystem link control".

[11] GSM 05.56: "Digital cellular telecommunications system (Phase 2+), GSM Cordless Telephony System Phase 1 CTS FP radio sub-system".

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

[13] GSM 11.14: "Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface ".

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

3 Definitions, abbreviations and symbols

3.1 Definitions

For the purposes of the present document, the following definition applies. For further information and definitions refer to GSM 01.02 [1] and GSM 11.11 [12].

CTS session: That part of the card session dedicated to the CTS operation.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply, in addition to those listed in GSM 01.04 [2] and GSM 11.11 [12]:

B5	CTS message authentication algorithm (for the authentication of the CTS-FPE by the CTS-SN)
CTS	Cordless Telephony System
CTS_MS_Max_TXPWR:	Maximum Output Power at CTS-MS
CTS_RXLEV_ACCESS_MIN:	Minimum received signal level to access CTS FP
CTSBCH	CTS-Beacon Channel
CTS-FP	CTS-Fixed Part (comprises a CTS-FPE and a FP-SIM)
CTS-FPE	CTS-Fixed Part Equipment
CTSMSI	Temporary Identity of a CTS MS for a given CTS FP
CTS-SN	CTS-Service Node
FP	Fixed Part
FPBI	Fixed Part Beacon Identity
FP-SIM	Fixed Part SIM
IFPEI	International Fixed Part Equipment Identity
Ka	local Authentication Key

Ki_{FP}	CTS Subscriber authentication key; the cryptographic key used by the authentication algorithm, A3, and cipher key generator, A8
Kop	Cryptographic key; used by the cipher B5
MS-SIM	Mobile Station SIM

3.3 Symbols

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

'0' to '9' and 'A' to 'F'	The sixteen hexadecimal digits

4 Specification of the Fixed Part Subscriber Identity Module

4.1 Physical characteristics

GSM 11.11 [12] and GSM 11.12 [14] applies.

4.2 Electronic signals and transmission protocols

GSM 11.11 [12] applies.

4.3 Logical Model

GSM 11.11 [12] applies with the following additional files IDs reserved for use by CTS:

Dedicated Files:

- operational use:

  '7F 23' ($DF_{FP\ CTS}$)

Elementary Files:

- administration use:

  '2F E2' (EF_{ICCID}) is a common file between a GSM SIM and a FP-SIM.

4.4 Security features

The security aspects of CTS are described in the normative references GSM 03.20 , Annex E [5]. This clause gives information related to security features supported by the FP-SIM to enable the following:

- authentication of the CTS subscriber identity to the network;
- file access conditions.

4.4.1 CTS-FPE Authentication for local security system

This subclause describes the authentication mechanism which are invoked by the fixed network interface for operator control on the CTS system. For the specification of the corresponding procedures across the FP-SIM/CTS-FPE interface see clause 4.8.

The CTS-SN sends a Random Number (RAND) to the CTS-FPE. The CTS-FPE passes the RAND to the FP-SIM in the command RUN GSM ALGORITHM. The FP-SIM returns the Kop value to the CTS-FPE which are derived using the algorithms and processes given below. Then the CTS-FPE performs the authentication using Kop and a fixed value to generate the signature SRES. CTS-FPE sends SRES to the network. The fixed network compares this value with the value of SRES which it calculates by itself. The comparison of these SRES values provides the authentication.

A subscriber authentication key Ki_{FP} is used in this procedure. This key Ki_{FP} has a length of 128 bits and is stored within the FP-SIM in the same way Ki is used in the SIM card for GSM authentication.

4.4.2 Algorithms and processes

The names and parameters of the algorithms supported by the FP-SIM are defined in GSM 03.20, Annex E [5]. These are:

- Algorithm A3 to generate the first part of the key Kop (Kop1);
- Algorithm A8 to generate the second part of the key Kop (Kop2).

These algorithms may exist either discretely or combined (into A38) within the FP-SIM. In either case the output on the FP-SIM/CTS-FPE interface is 12 bytes. The inputs to both A3 and A8, or A38, are Ki_{FP} (128 bits) internally derived in the FP-SIM, and RAND (128 bits) across the FP-SIM/CTS-FPE interface. The output is the concatenation of Kop1 (32 bits)/Kop2 (64 bits) to produce Kop the coding of which is defined in the command RUN GSM ALGORITHM in subclause 4.6.1.

4.5 Description of the functions

GSM 11.11 [12] applies with the following additional specification.

4.5.1 RUN GSM ALGORITHM

This function is used during the procedure for authenticating the CTS-FPE to a CTS-SN and to calculate a cipher key. The card runs the specified algorithms A3 and A8 using a 16 byte random number and the subscriber authentication key Ki_{FP}, which is stored in the FP-SIM. The function returns the key Kop.

The function shall not be executable unless $DF_{FP\ CTS}$ or any sub-directory under $DF_{FP\ CTS}$ has been selected as the Current Directory. The CHV1 shall be always disabled.

Input:

- RAND.

Output:

- Kop.

4.6 Description of the commands

GSM 11.11 [12] applies.

4.6.1 RUN GSM ALGORITHM

COMMAND	CLASS	INS	P1	P2	P3
RUN GSM ALGORITHM	'A0'	'88'	'00'	'00'	'10'

Command parameters/data:

Byte(s)	Description	Length
1 - 16	RAND	16