



EUROPEAN
TELECOMMUNICATION
STANDARD

ETS 300 509

September 1994

Source: ETSI TC-SMG

Reference: GSM 02.17

ICS: 33.060.20

Key words: European digital cellular communications system, Global System for Mobile communications (GSM)

**European digital cellular telecommunications system (Phase 2);
Subscriber Identity Modules (SIM)
Functional characteristics
(GSM 02.17)**

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

X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

Copyright Notification: No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 1994. All rights reserved.

Contents

Foreword	5
1 Scope	7
2 Normative references	7
3 Definitions and abbreviations	8
3.1 Definitions	8
3.2 Abbreviations	8
4 General	9
4.1 Characteristics	10
4.1.1 ID-1 SIM	10
4.1.2 Plug-in SIM	10
4.2 Phases of operation	10
4.2.1 Administrative management phase	10
4.2.2 GSM network operation phase	11
5 Security features	11
5.1 SIM interface	11
5.2 SIM data	11
5.3 Algorithms and subscriber authentication key	12
5.4 Administrative management phase	12
5.5 Subscriber data stored in ME	12
5.6 PIN management	12
5.7 SIM removal	13
6 SIM information storage requirements	13
6.1 Mandatory storage	13
6.2 Optional storage	13
7 Mobile Equipment accepting both ID-1 and Plug-in SIMs	14
History	15

Blank page

Foreword

This European Telecommunication Standard (ETS) has been produced by the Special Mobile Group (SMG) Technical Committee (TC) of the European Telecommunications Standards Institute (ETSI).

This ETS defines the functional characteristics of the Subscriber Identity Module (SIM) of Mobile Stations (MS) within the European digital cellular telecommunications system (Phase 2).

This ETS corresponds to GSM technical specification GSM 02.17 version 4.3.3.

The specification from which this ETS has been derived was originally based on CEPT documentation, hence the presentation of this ETS may not be entirely in accordance with the ETSI/PNE rules.

Reference is made within this ETS to GSM-TSs (NOTE).

NOTE: TC-SMG has produced documents which give the technical specifications for the implementation of the European digital cellular telecommunications system. Historically, these documents have been identified as GSM Technical Specifications (GSM-TSs). These TSs may have subsequently become I-ETTs (Phase 1), or ETSS (Phase 2), whilst others may become ETSI Technical Reports (ETRs). GSM-TSs are, for editorial reasons, still referred to in GSM ETSS.

Blank page

1 Scope

This Technical Specification (TS) defines the functional characteristics and requirements of the Subscriber Identity Module (SIM) for use in GSM and DCS 1800 applications. All references to GSM shall apply equally to DCS 1800 unless otherwise stated.

The SIM is the entity that contains the identity of the subscriber. When placed in a Mobile Equipment (ME), together they become a Mobile Station (MS) which may then register onto a GSM network.

The primary function of the SIM in conjunction with a GSM network is to authenticate the validity of an MS when accessing the network. In addition it provides a means to authenticate the user and may also store other subscriber-related information. Subscription entitlements are stored not in the SIM, but in the network.

If the SIM functionality is incorporated into a multi-application ETSI/TE9 card, the GSM application may be used in other telecommunication applications.

In addition SIMs are permitted to contain non-GSM functionality. In the case of multi-application cards, this TS defines just the GSM application.

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] GSM 01.02 (ETR 099): "European digital cellular telecommunication system (Phase 2); General description of a GSM Public Land Mobile Network (PLMN)".
- [2] GSM 01.04 (ETR 100): "European digital cellular telecommunication system (Phase 2); Definitions, abbreviations and acronyms".
- [3] GSM 02.03 (ETS 300 502): "European digital cellular telecommunication system (Phase 2); Teleservices supported by a GSM Public Land Mobile Network (PLMN)".
- [4] GSM 02.07 (ETS 300 505): "European digital cellular telecommunication system (Phase 2); Mobile Station (MS) features".
- [5] GSM 02.09 (ETS 300 506): "European digital cellular telecommunication system (Phase 2); Security aspects".
- [6] GSM 02.11 (ETS 300 507): "European digital cellular telecommunication system (Phase 2); Service accessibility".
- [7] GSM 02.24 (ETS 300 510): "European digital cellular telecommunication system (Phase 2); Description of Charge Advice Information (CAI)".
- [8] GSM 02.30 (ETS 300 511): "European digital cellular telecommunication system (Phase 2); Man-Machine Interface (MMI) of the Mobile Station (MS)".
- [9] GSM 03.20 (ETS 300 534): "European digital cellular telecommunication system (Phase 2); Security related network functions".
- [10] GSM 03.40 (ETS 300 536): "European digital cellular telecommunication system (Phase 2); Technical realisation of the Short Message Service (SMS) Point-to-Point (PP)".

- [11] GSM 03.41 (ETS 300 537): "European digital cellular telecommunication system (Phase 2); Technical realisation of the Short Message Service Cell Broadcast (SMSCB)".
- [12] GSM 11.11 (ETS 300 608): "European digital cellular telecommunication system (Phase 2); Specification of the Subscriber Identity Module-Mobile Equipment (SIM-ME) interface".
- [13] ISO 7816-1, 1987: "Identification cards - Integrated circuit(s) cards with contacts, Part 1: Physical characteristics".
- [14] ISO 7816-2, 1988: "Identification cards - Integrated circuit(s) cards with contacts, Part 2: Dimensions and locations of the contacts".
- [15] CCITT Recommendation E.118, (1988): "Automated international telephone credit card system".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this standard, the following definitions apply. For further information and abbreviations refer to TS GSM 01.02 [1] and TS GSM 01.04 [2].

Cipher Key: a key used in conjunction with an algorithm (A5) to cipher user and signalling data (see TS GSM 03.20 [9]).

GSM or DCS 1800 application: A set of security mechanisms, files, data and protocols required by GSM or DCS 1800.

IC card SIM: obsolete term for ID-1 SIM.

ID-1 SIM: the SIM having the format of an ID-1 card (see ISO/IEC 7816-1 [13]).

Plug-in SIM: a second format of SIM (specified in Clause 4).

3.2 Abbreviations

For the purposes of this standard the following abbreviations apply.

A3	Algorithm 3, authentication algorithm; used for authenticating the subscriber
A5	Algorithm 5, cipher; used for enciphering/deciphering data
A8	Algorithm 8, cipher key generator; used to generate Kc
ADN	Abbreviated Dialling Number
BCCH	Broadcast Control CHannel
CCITT	The International Telegraph and Telephone Consultative Committee (now also known as ITU Telecommunications Standardization sector)
CHV	Card Holder Verification Information; access condition used by the SIM for the verification of the identity of the user (for GSM this is the PIN)
DCS	Digital Cellular System
ETSI	European Telecommunications Standards Institute
FDN	Fixed Dialling Number

GSM	Global System for Mobile communications
HPLMN	Home PLMN
IC	Integrated Circuit
IEC	International Electrotechnical Commission
IMSI	International Mobile Subscriber Identity
ISO	International Organization for Standardization
Kc	cryptographic key; used by the cipher, A5
Ki	subscriber authentication key; the cryptographic key used by the authentication algorithm, A3, and cipher key generator, A8
LAI	Location Area Information; information indicating a cell or a set of cells
LND	Last Number Dialed
ME	Mobile Equipment
MMI	Man Machine Interface
MS	Mobile Station
MSISDN	Mobile Station international ISDN number
PIN/PIN2	Personal Identification Number / Personal Identification Number 2 (common names for CHV1 and CHV2, respectively)
PLMN	Public Land Mobile Network
PUK/PUK2	PIN Unlocking Key / PIN Unlocking Key 2 (common names for UNBLOCK CHV1 and UNBLOCK CHV2, respectively)
SIM	Subscriber Identity Module
SMS	Short Message Service
SSC	Supplementary Service Control string
TE9	Terminal Equipment 9 (ETSI sub-technical committee)
TMSI	Temporary Mobile Subscriber Identity
TS	Technical Specification
UNBLOCK CHV1/2	value to unblock CHV1/CHV2

4 General

A GSM MS comprises an ME and a SIM. The SIM is a removable module. The SIM contains the International Mobile Subscriber Identity (IMSI) which unambiguously identifies a subscriber. Without a valid IMSI, GSM service is not accessible (except emergency calls, as defined in TS GSM 02.03 [3]).

The user interface (MMI) of the ME related to SIM operations is defined in TS GSM 02.30 [8].

TS GSM 02.09 [5] specifies a security function for authenticating the SIM. This function, which is mandatory for any MS, is based on a cryptographic algorithm, A3, and a secret subscriber authentication key, Ki, both of which are located in the SIM.

The SIM provides storage of subscriber related information. This data is of three types:

- data fixed during administrative phase; e.g. IMSI, subscriber authentication key, access control class;
- temporary network data; e.g. TMSI, LAI, Kc, Forbidden PLMNs;
- service related data; e.g. Language Preference, Advice of Charge.

The SIM contains a personal identification number (PIN) (see Clause 5) to provide protection against unauthorised use. For some optional features the use of a second personal identification number (PIN2) is required. PIN(s) shall be stored and verified within the SIM.

4.1 Characteristics

Two physical types of SIM are specified. These are the "ID-1 SIM" and the "Plug-in SIM".

The physical characteristics of both types of SIM are defined in TS GSM 11.11 [12].

The logical and electrical interface of the SIM is defined in TS GSM 11.11 [12] and is identical for both types of SIM.

The information on the exterior of either SIM should include at least the individual account identifier and the check digit of the IC Card Identification (see CCITT Recommendation E.118 [15]).

4.1.1 ID-1 SIM

Format and layout of the ID-1 SIM shall be in accordance with ISO 7816-1,2 [13, 14]). The card shall have a polarisation mark, as defined in TS GSM 02.07 [4], which indicates how the user should insert the card into the ME.

SIMs may be embossed (see TS GSM 11.11 [12]).

4.1.2 Plug-in SIM

The Plug-in SIM is smaller than the ID-1 SIM and has dimensions as defined in TS GSM 11.11 [12]. It is intended to be semi-permanently installed in the ME.

4.2 Phases of operation

4.2.1 Administrative management phase

GSM administrative management phase may be entered at any time, to bring in or change data not accessible by the subscriber in GSM operational phase. Only by specific administrative authentication mechanisms and commands can the administrative phase be entered and administrative functions be performed. The specification of administrative operations and the parties responsible for them are outside the scope of this TS.

The different types of administrative phases which may occur during the lifetime of a SIM are:

- production;
- (pre)(re)personalisation;
- distribution.

Following production a SIM contains at least the authentication algorithm and the operating system necessary for (pre)personalisation.

Prepersonalisation, personalisation and repersonalisation are processes during which subscription data, e.g. IMSI, and subscriber data are entered into or updated in the SIM. The split between these processes and adoption of appropriate security measures is dependent upon the chosen administrative management structure.

For example, the following parties may have responsibilities during the administrative phase as follows:

- SIM manufacturer: card production;
- SIM issuer: SIM configuration;
- Service activator: activating the SIM on the GSM network;
- Delivery party: programming of subscriber data and distribution of card to subscriber.

These parties may be separate organisations or combined, and the activities merged; e.g. SIM issue, Service Activation and Delivery may all be the responsibility of a network operator.

4.2.2 GSM network operation phase

Once a SIM has been personalised with all data required for GSM network operation, the GSM network operation phase is entered.

5 Security features

The security aspects of GSM are defined in TS GSM 02.09 [5] and TS GSM 03.20 [9].

This clause defines the security attributes to be supported by the SIM which are:

- authentication algorithm (A3);
- subscriber authentication key (Ki);
- cipher key generation algorithm (A8);
- cipher key (Kc);
- control of access to data stored, and functions performed, in the SIM.

An algorithm A38 may perform the combined functions of A3 and A8.

5.1 SIM interface

Other commands than those specified in TS GSM 11.11 [12] are only allowed to be executed if they do not interfere with the correct functioning of the GSM application.

If the GSM application is one of several applications on a multi-application IC card, then the other applications shall have no means of unauthorised access to the GSM application.

5.2 SIM data

Actions, e.g. read, update, on SIM data shall be controlled by access conditions, which shall be satisfied before the action can be performed. The access conditions and the data to which they apply are defined in TS GSM 11.11 [12].

5.3 Algorithms and subscriber authentication key

All reasonable steps shall be taken to ensure that the algorithms (A3 and A8) and subscriber authentication key (Ki) cannot be read, altered, manipulated or bypassed in such a way as to reveal secret information.

All MS processes which require the use of the subscriber authentication key shall be performed internally by the SIM.

5.4 Administrative management phase

This TS does not define the security requirements of the administrative phase but precautions shall be taken to protect the integrity of subscriber related secret information.

5.5 Subscriber data stored in ME

Subject to the exception below, all subscriber related information transferred into the ME during GSM network operations shall be deleted from the ME after removal of the SIM or deactivation of the MS.

Subscriber related security codes (e.g. PIN and PUK) may be kept in the ME during the execution of the appropriate SIM/ME interface procedure (e.g. verifying or changing a PIN). They shall be deleted from the ME immediately after completion of the procedure.

Optionally, an ME may retain some less security critical data at SIM removal or MS switch-off. Such data are SMS, ADN/SSC, FDN/SSC and LND. These data, when stored in the ME, shall only be readable/retrievable if the same SIM is reactivated (as determined by the IMSI). If the IMSI is retained in the ME for this purpose it shall be stored securely and shall not be able to be read out.

ADN/SSC storage may also exist in the ME. These ADN/SSC stored in the ME, which have not been transferred from a SIM during a card session, are not subject to the above security restriction.

5.6 PIN management

The GSM SIM shall support the use of Card Holder Verifications (CHV) to authenticate the user to the card e.g. to provide protection against the use of stolen cards. For the SIM the CHV information takes the form of a numeric PIN of 4 to 8 decimal digits. An initial PIN is loaded during the administrative management phase.

A PIN disabling function may exist. This function may be inhibited at card issue. In this case the subscriber shall always use the PIN. Otherwise the subscriber may decide whether or not to make use of the PIN function. If disabled, the PIN remains disabled until the subscriber specifically re-enables PIN checking.

Depending on the requirements of the SIM issuer, and subject to the features incorporated in the SIM, e.g. FDN, a second Subscriber PIN (PIN2) may be provided. Like PIN, PIN2 shall also consist of 4 to 8 (decimal) digits loaded during the administrative phase. There shall be no provision for the subscriber to disable PIN2.

Following correct PIN or PIN2 presentation, the ME may perform functions, and actions on SIM data, protected by the relevant PIN access condition.

If an incorrect PIN or PIN2 is entered, an indication is given to the user. After three consecutive incorrect entries the relevant PIN is blocked, i.e. functions, and actions on data, protected by the PIN access condition are no longer possible, even if between attempts the SIM has been removed or the MS has been switched off. Once a PIN is blocked, further PIN verifications cannot be performed.

The SIM shall support a mechanism for unblocking a blocked PIN. Unblocking of a PIN is performed using the relevant function defined in TS GSM 11.11 [12] in association with the relevant PIN Unblocking Key (PUK/PUK2).

PIN and PIN2 (length and value) shall be changeable by the subscriber following correct entry of either the current PIN/PIN2 or PUK/PUK2 as appropriate.

On a SIM handling both PIN and PIN2, there is no hierarchical relationship between them, e.g. correct presentation of PIN2 does not allow actions to be performed which require presentation of PIN, and *vice versa*.

The PUKs shall consist of 8 decimal digits loaded during the administrative management phase and are not changeable by the user. If an incorrect PUK is presented, an indication is given to the user. After 10 consecutive incorrect entries, the PUK is itself blocked, even if between attempts the SIM has been removed or the MS has been switched off. Unblocking of the relevant PIN is now impossible.

It shall not be possible to read the PIN(s) or PUK(s).

5.7 SIM removal

If the SIM is removed from the MS during a call, the call shall be terminated immediately.

6 SIM information storage requirements

The SIM shall contain information elements for GSM network operations. The SIM may contain information elements related to the mobile subscriber, GSM services and PLMN related information, e.g. PLMN Selector.

6.1 Mandatory storage

The SIM shall provide storage capability for the following:

- Administrative information: indicates mode of operation of the SIM, e.g. normal, type approval;
- IC card identification: a number uniquely identifying the SIM and the card issuer;
- SIM service table: indicates which optional services are provided by the SIM;
- International Mobile Subscriber Identity (IMSI);
- Location information: comprising Temporary Mobile Subscriber Identity (TMSI), Location Area Information (LAI), Current value of Periodic Location Updating Timer (T3212) and the Location update status;
- Cipher key (Kc) and cipher key sequence number;
- BCCH information: list of carrier frequencies to be used for cell selection;
- Access control class(es): (see TS GSM 02.11 [6]);
- Forbidden PLMNs: (see TS GSM 02.11 [6]);
- HPLMN search period: used to control the time interval between HPLMN searches (see TS GSM 02.11 [6]);
- Language preference; subscriber preferred language(s) of MMI;
- Phase identification.

Location Information, Cipher Key and Cipher Key Sequence Number shall be updated on the SIM after each call termination and when the MS is correctly deactivated in accordance with the manufacturer's instructions.

In addition the SIM shall manage and provide storage for the following information in accordance with the security requirements of Clause 5:

- PIN;
- PIN enabled/disabled indicator;
- PIN error counter;
- PUK;
- PUK error counter;
- Subscriber authentication key.

6.2 Optional storage

The SIM may provide storage capability for the following:

- PLMN selector: for automatic PLMN selection (see TS GSM 02.11 [6]);
- Cell Broadcast Message Identifier Selection: (see TS GSM 03.41 [11]);
- Abbreviated Dialling Numbers/Supplementary Service Control: (see TS GSM 02.30 [8]);
- Fixed Dialling Numbers/Supplementary Service Control:(see TS GSM 02.07 [4]);
- MSISDN number(s): for subscriber number(s);
- Last number(s) dialled: (see TS GSM 02.07 [4]);
- Capability configuration parameters: provides the parameters of required bearer capabilities associated with dialling numbers;
- Called party subaddress: (see TS GSM 02.07 [4]);
- Short messages and associated parameters: (see TS GSM 03.40 [10]);
- Accumulated call meter, Accumulated call meter maximum value and Price per unit & currency table:(see TS GSM 02.24 [7]).

In addition, if the SIM supports PIN2, the following information shall be managed and stored by the SIM in accordance with the security requirements of Clause 5:

- PIN2;
- PIN2 error counter;
- PUK2;
- PUK2 error counter.

7 Mobile Equipment accepting both ID-1 and Plug-in SIMs

An ME able to accept a Plug-in SIM may also have provision for accepting an ID-1 SIM. If both SIMs are present the ID-1 SIM takes precedence.

If the ID-1 SIM is inserted during a call which was previously established using the Plug-in SIM, the ID-1 SIM shall take precedence after the call is terminated.

If a SIM is removed, any call in progress made using that SIM is terminated immediately. All security considerations of Clause 5 now relate to the remaining SIM and network operation resumes with the identity of the remaining SIM.

History

Document history	
September 1994	First Edition
October 1995	Converted into Adobe Acrobat Portable Document Format (PDF)