ETSI TS 142 017 V4.0.0 (2001-03)

**Digital cellular telecommunications system (Phase 2+);
Subscriber Identity Modules (SIM);
Functional characteristics
(3GPP TS 42.017 version 4.0.0 Release 4)**

**GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS**

Reference
RTS/TSGT-0342017Uv4

Keywords
GSM

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

ETSI

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 Technical Specification (TS) has been produced by the ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under www.etsi.org/key .

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

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

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

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

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document defines the functional characteristics and requirements of the Subscriber Identity Module (SIM) for use in Digital Cellular Telecommunications System (GSM) applications. All references to GSM shall apply equally to any band specified for GSM 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 or applications. Subscription entitlements are stored not in the SIM, but in the network.

If the SIM functionality is incorporated into a multi-application 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, the present document defines just the GSM application.

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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[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 02.03: "Digital cellular telecommunications system (Phase 2+); Teleservices supported by a GSM Public Land Mobile Network (PLMN)".

[4]   GSM 02.07: "Digital cellular telecommunications system (Phase 2+); Mobile Station (MS) features".

[5]   GSM 02.09: "Digital cellular telecommunications system (Phase 2+); Security aspects".

[6]   GSM 02.11: "Digital cellular telecommunications system (Phase 2+); Service accessibility".

[7]   not used.

[8]   GSM 02.30: "Digital cellular telecommunications system (Phase 2+); Man-Machine Interface (MMI) of the Mobile Station (MS)".

[9]   GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[10]   not used.

[11]   not used.

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

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

[14]   ISO/IEC 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".

[16]   GSM 11.12 (ETS 600 641): "Digital cellular telecommunication system (Phase 2); Specification of the 3 Volt Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

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

3   Definitions and abbreviations

3.1   Definitions

For the purposes of the present document, the following terms and definitions apply. For further information and abbreviations refer to GSM 01.02 [1] and GSM 01.04 [2].

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

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

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 the present document, 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. The GSM SIM contains two CHVs: CHV1 is the primary access control mechanism, and CHV2 allowing a different level of access.
FDN   Fixed Dialling Number
HPLMN   Home PLMN
IC   Integrated Circuit
IEC   International Electrotechnical Commission
IMSI   International Mobile Subscriber Identity
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 Dialled
ME   Mobile Equipment

MMI	Man Machine Interface
MS	Mobile Station
MSISDN	Mobile Station international ISDN number
PLMN	Public Land Mobile Network
SIM	Subscriber Identity Module
SMS	Short Message Service
SSC	Supplementary Service Control string
TMSI	Temporary Mobile Subscriber Identity

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 GSM 02.03 [3]).

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

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 Card Holder Verification information (CHV1 - see clause 5) to provide protection against unauthorized use. For some optional features, the use of a second CHV (CHV2) is required. CHV(s) shall be stored and verified within the SIM.

The SIM may also contain applications which use the features defined in the SIM Application Toolkit specification GSM 11.14 [17]

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 GSM 11.11 [12].

The logical and electrical interface of the SIM is defined in GSM 11.11 [12] and GSM 11.12 [16] 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 polarization mark, as defined in GSM 02.07 [4], which indicates how the user should insert the card into the ME.

SIMs may be embossed (see 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 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 the present document.

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

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

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

Prepersonalization, personalization and repersonalization 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 organizations 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 personalized 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 GSM 02.09 [5] and 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 GSM 11.11 [12] and GSM 11.14 [17] are only allowed to be executed if they do not interfere with the correct functioning of the GSM application. The execution of GSM commands as specified in GSM 11.11 [12] shall always take precedence over any SIM Application Toolkit commands as specified in GSM 11.14 [17].

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

The present document 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, deactivation of the MS, or following an electrical reset of the SIM. This includes any data that was transferred to the ME by SIM Application Toolkit commands.

Subscriber related security codes (e.g. CHV and Unblock CHV) may be kept in the ME during the execution of the appropriate SIM/ME interface procedure (e.g. verifying or changing a CHV). 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, LND etc. 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.

Storage for other data such as ADN/SSC, SMS etc., storage may also exist in the ME. These data 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 CHV 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 CHV of 4 to 8 decimal digits. An initial CHV is loaded during the administrative management phase.

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

Depending on the requirements of the SIM issuer, and subject to the features incorporated in the SIM, e.g. FDN, a second Subscriber CHV (CHV2) may be provided. Like CHV, CHV2 shall also consist of 4 to 8 (decimal) digits loaded during the administrative phase. There shall be no provision for the subscriber to disable CHV2.

Following correct CHV or CHV2 presentation, the ME may perform functions, and actions on SIM data, protected by the relevant CHV access condition.

If an incorrect CHV or CHV2 is entered, an indication is given to the user. After three consecutive incorrect entries the relevant CHV is blocked, i.e. functions, and actions on data, protected by the CHV access condition are no longer possible, even if between attempts the SIM has been removed or the MS has been switched off. Once a CHV is blocked, further CHV verifications cannot be performed.

There shall be two possible methods of handling CHVs that are blocked. Cards may, if the CHV is disabled, allow the CHV to become blocked without re-enabling the CHV, such that use of the GSM service is still possible. Conversely,

cards may, if the CHV is disabled, re-enable the CHV if it becomes blocked. The method chosen is a matter for the card issuer.

The SIM shall support a mechanism for unblocking a blocked CHV. Unblocking of a CHV is performed using the relevant function defined in GSM 11.11 [12] in association with the relevant CHV Unblocking Key (Unblock CHV/Unblock CHV2).

CHV and CHV2 (length and value) shall be changeable by the subscriber following correct entry of either the current CHV/CHV2 or Unblock CHV/Unblock CHV2 as appropriate.

On a SIM handling both CHV and CHV2, there is no hierarchical relationship between them, e.g. correct presentation of CHV2 does not allow actions to be performed which require presentation of CHV, and *vice versa*.

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

It shall not be possible to read the CHV(s) or Unblock CHV(s).

5.7 SIM removal

If the SIM is removed from the MS during a call, the call shall be terminated immediately as defined in GSM 11.11 [12].

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 GSM 02.11 [6]).
- Forbidden PLMNs: (see GSM 02.11 [6]).
- HPLMN search period: used to control the time interval between HPLMN searches (see 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:

- CHV;
- CHV enabled/disabled indicator;
- CHV error counter;
- Unblock CHV;
- Unblock CHV error counter;
- Subscriber authentication key (Ki).

6.2 Optional storage

The SIM may provide storage capability for optional datafields required to support optional GSM features and services. Refer to GSM 11.11 [12] for descriptions of optional datafields.

If the SIM supports CHV2, the following information shall be managed and stored by the SIM in accordance with the security requirements of clause 5:

- CHV2;
- CHV2 error counter;
- Unblock CHV2;
- Unblock CHV2 error counter.

If the SIM supports the SIM Application Toolkit as specified in GSM 11.14 [17], the SIM shall provide storage for the SIM Applications and data associated with those application.

7 Mobile Equipment accepting multiple SIMs

For Mobile Equipment, which accepts multiple SIMs, the user shall have the ability, via MMI, to select their preference for SIM Card Reader selection. The preferences shall initially have a default setting which the user can adjust. Once adjusted the preferences become the default setting.

If a non preferred SIM Card Reader is in use and a SIM becomes available in a preferred SIM Card Reader, the user shall be offered the choice to select the preferred SIM.

On power up, the ME will attempt to use the user preferred choice, but, if this is not available, the ME will use any other available SIM.

The use of a default setting will remove the necessity for the majority of users to access this MMI feature.

If a new SIM is inserted in the preferred reader during a call, the user shall be offered the ability to select the new SIM after the call is terminated.

If the active SIM is removed, any network transaction using that SIM shall be terminated immediately, as defined in GSM 11.11 [12]. If another SIM is available, it shall be selected.

The ME shall indicate to the user which SIM is active.

Annex A (informative): Change history

This annex lists all change requests approved for this document since the first phase 2 version was approved by ETSI SMG.

Meeting	Plenary tdoc	WG Doc	VERS	CR	RV	PH	CAT	SUBJECT	Resulting Version
s02	167/92		4.0.0	016	1	2	D	Editorial update	4.1.0
s05	98/93		4.1.0	017	1	2	C	Last Dialled Number	4.2.0
	98/93			018		2	C	SMS CB parameter on SIM	
s08	538/93		4.2.0	019		2	F	Polarisation mark	4.3.0
	539/93			020		2	F	Storage of CHV in ME	
	539/93			021		2	F	Execution of non GSM commands during a GSM session	
s20	*At SMG #20, it was decided that all specifications that existed only as a phase 2 version should also be made available as a phase 2+ specification. This applied to GSM 02.17. It was sent on OAP in December 1996 at version 5.0.0 and published in April 1997 as version 5.0.1 Both 5.0.0 and 5.0.1 are identical in content to version 4.3.0*								
s26	98-0403	98p226	5.0.1	A002		R98	C	Operation of ME with multiple card readers	7.0.0
s27	98-0672	98p083	7.0.0	A001		R98	B	Alignment of GSM 02.17 with GSM 11.11 and GSM 11.14	7.1.0
s30	P-99-668	9-99-272	7.1.1	A004		R99	D	Removal of references to specific GSM bands	8.0.0
s32	*At SMG #32, all remaining GSM specifications were transferred to the 3GPP. Further entries in this table refer to 3GPP meetings*								
TP-11	*At TSG-T #11, it was agreed that all existing release 99 specifications should be reissued as release 4 specifications so as to create a complete set of release 4 specifications. Further more, it was agreed to change the specification number of all GSM-only specifications from AA.BB to (AA+40).0BB. Thus GSM 02.17 changed to 3GPP TS 42.017. At the same time, the version numbering scheme was harmonised with 3G specifications so that all release 4 specifications have a version number 4.x.y. The contents of TS 42.017 v4.0.0 are identical to GSM 02.17 v8.0.0*								4.0.0

History

Document history		
V4.0.0	March 2001	Publication