ETSI/TC SMG
Released by : ETSI/PT 12
Release date: February 1992

RELEASE NOTE

Recommendation GSM 02.17

Subscriber Identity Modules, Functional Characteristics

Previously distributed version : 3.2.0 (Release 1/90)
New Released version February 92 : 3.2.0 (Release 92, Phase 1)

1. Reason for changes

No changes since the previously distributed version.

ETSI/GSM

Released by: ETSI PT12

Date: February 1992

Recommendation: GSM 02.17

Title: SUBSCRIBER IDENTITY MODULES, FUNCTIONAL CHARACTERISTICS

List of contents:

Original language: English

Number of pages: 11

1. SCOPE

This document describes the functional characteristics of the Subscriber Identity Module (SIM). It is a requirement that the SIMs are electrically (regarding the connections), logically and functionally standardized for both types as mentioned below for all GSM MS's. Both types will only differ in physical respect, however the physical characteristics are standardized per type. Recommendation GSM 11.11 describes the (technical) SIM specifications.

Mobile service may be one of the applications of a multiservice IC card. All specifications of the IC card in this recommendation refer to the part of the IC card which is specific for GSM mobile services.

It is foreseen that SIM functions will have to be updated in course of time. Upwards compatibility shall be assured with regard to the standardization of the network interface functions of the SIM via the ME and with regard to the user related SIM functions on the SIM-ME interface.

2. GENERAL

2.1. Description

The International Mobile Subscriber Identity (IMSI) is the information which uniquely identifies a subscriber to the GSM PLMN. Mobile stations can only be operated if a valid IMSI is present (except for emergency calls when it is allowed according to Rec. GSM 02.03). According to Rec. GSM 02.09, the MS must contain a security function for authentication of the subscriber identity: a secret authentication key and a cryptographic algorithm. The Subscriber Identity Module is the module which contains all the processes involving the authentication key. The SIM also contains the IMSI, and mobile subscriber related information. The SIM shall have a clearly defined physical and logical interface with the outside world.

In all cases a PIN may be used to provide protection against unauthorized use of the SIM. For security reasons the PIN must be stored and checked within the SIM.

The SIM is a removable module. The SIM shall provide storage of subscriber related temporary data (TMSI, LAI, Kc, Timervalue).

2.2. Definitions

The SIM is a removable module which is meant to be inserted either whenever the subscriber wants to use the MS and may be removed when the MS is unattended or a SIM installed in the MS at subscription time. Two variants are introduced:

IC card SIM and plug-in SIM

1. IC card SIM

   A module, the interface of which with the outside world is in accordance with ISO standards on IC cards (ISO 7816 series). The SIM may be a part of a multi service card, of which GSM mobile telecommunication is one of the applications.

2. Plug-in SIM

   A dedicated module to be fully standardized within the GSM system. It is intended to be semi-permanently installed in the ME.

Mobile Equipment (ME)

The ME is the Mobile Station (MS) without the SIM.

GSM network operation

GSM network operations are operations during set-up, active- and clearing phase of a call. When used in the ME, the SIM shall provide the following functions when it is in GSM network operation:

- storage of subscriber related security information (e.g. IMSI, keys) of Rec. GSM 02.09, and implementation of authentication and cipher key generation mechanisms (algorithms A3 and A8) of Rec. GSM 03.20;

- User PIN operation (if a PIN is required) and management;

- management of mobile subscriber related information.

GSM network operation is only possible when the SIM has a valid IMSI.

GSM administrative management operation

GSM administrative management operations are all operations needed to provide GSM subscribers with a valid SIM, allowing access to GSM services. GSM administrative management operations have to deal with the different phases that occur during the lifetime of a SIM. A SIM life may consists of the following phases:

- production;
- distribution;
- (pre)personalization;
- repersonalization;
- blocking.

Application data file (ADF)

When the IC card SIM is part of a multiservice IC card the set of data (including programs) related to GSM is organized into one specific Application Data File called GSM ADF.

Relevant parties

Regarding GSM administrative management operation, the following parties are identified:

1. SIM manufacturer: responsible for serial number and transportation code and security algorithm;
2. SIM issuer: creates GSM ADF;
3. Service activator: responsible for management of Ki, IMSI, subscriber number, and for enabling network access;
4. Delivery party: responsible for programming of subscriber data;
5. GSM Subscriber.

3. SIM REQUIREMENTS

3.1. Security Requirements

3.1.1. General

The authentication key, and all mobile subscriber related secret information must be protected at all times, not only when it is conveyed from the key management center to the SIM but also during GSM network operation of the SIM. Therefore the SIM functions and the data must be kept in a physically and logically secure environment (see Rec. GSM 02.09). The SIM shall have a clearly defined physical and logical interface with the outside world.

Security also depends on the organization of the SIM memory and on the management of subscriber related data within the ME. For security reasons all reasonable steps must be taken to guarantee that algorithms A3 and A8 cannot be altered, bypassed or manipulated in such a way to reveal secret information. Modifications, updates and changes regarding the security functions of the SIM require a new SIM to be issued.

If the GSM ADF is one of several ADF's in a multiservice IC card, all other ADF's shall have no means of unauthorized accessing of any data of the GSM ADF.

3.1.2. Security in GSM network operation

No commands other than those specified shall be understood by the SIM in GSM network operations (when dealing with the GSM application in case of multi-application IC card SIM). The SIM must contain a mechanism that allows a responsible party to test (ref. Rec. GSM 11.11) the SIM for a correct implementation.

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.

3.1.3. PIN Management

The SIM must be able to handle a PIN, even if it will be never used. The PIN shall consists of 4 to 8 (numeric only) digits.

An initial PIN is loaded by the service activator at subscription time. Afterwards the PIN, as well as the length of the PIN, can be changed by the user as often as he likes. The user will be able to decide whether to make use of the PIN function, or not by using an appropriate SIM-ME function called PIN disabling function. This disabling is valid until the user specifically re-enables the PIN check.

This PIN disabling function can be inhibited at subscription time by a person authorized to do so by the network operator, i.e. the subscriber has no choice if the disabling function is inhibited but is forced to use the PIN.

If an incorrect PIN is entered, an indication is given to the user. After three consecutive incorrect entries the SIM is blocked, even if between attempts the SIM has been removed or the MS has been switched off. For unblocking see section 3.3.4.

3.2. Operational Requirements for GSM network operations

3.2.1. General

When using a SIM it is always possible to remove the SIM from the ME by an appropriate procedure (specified in Rec. GSM 11.11). In that case calls in progress will be immediately terminated according to the appropriate call clearing procedure.

When inserting the SIM (i.e. after answer to reset) all relevant subscriber related data shall be transferred from the SIM to the ME.

Subscriber related temporary data (e.g. TMSI, LAI, Kc,...) shall be stored on the SIM after each call termination and when the MS is correctly deactivated. Integrity of stored data is only guaranteed when the SIM is removed after a correct (that is to say according to the ME manufacturer instructions) deactivation of the MS.

Both types of SIM are, in GSM network operation, identical from the functional and logical (e.g. structure of messages, protocol) point of view. Each of the two types are fully standardized in order to guarantee unconditional interchangeability between SIMs of alike type, for each variant of MS for which they have been designed.

3.2.2. IC Card SIM

The IC card SIM requires an appropriate accepting device in the ME. The ISO international standards for the physical, electrical and logical characteristics apply. See Rec. GSM 11.11 for further details.

3.2.3. Plug-in SIM

One common interface for the plug-in SIM shall be standardized within GSM specify by its physical, electrical and logical characteristics. The plug-in SIM requires an appropriate connector in the ME.

3.3. Requirements For GSM Administrative Management

3.3.1. General

Administrative management of the SIM is the responsibility of the GSM PLMN operator. Only those aspects which may impact on other PLMN operators need to be standardized within GSM.

3.3.2. Distribution of SIMs

When a SIM is delivered by the SIM supplier it contains all functions necessary to operate or to be initialized to operate but it contains no authentication key and no IMSI. The SIM contains the authentication function including the algorithm.

3.3.3. Prepersonalization and Personalization of SIMs

Prepersonalization is assigning and loading a SIM with authentication key and IMSI, and is done using a prepersonalization key. Prepersonalization is done in a secure environment under responsibility of the service activator.

Personalization consists of associating subscriber data (e.g. directory number) to a prepersonalized SIM and performing the necessary programming and administration. This operation is performed at subscription time, either in a central management center or remotely in any location, using a personalization key. Personalization is done under the HPLMN operators responsibility.

3.3.4. Blocking/unblocking of SIM

Blocking of a SIM is to put it into a status which forbids GSM network operations. Unblocking is possible under the control of a personal unblocking key.

The personal unblocking key shall be numeric only, with 8 digits. If an incorrect one is entered, an indication is given to the user. After 10 consecutive incorrect entries the SIM is blocked, even if between attempts the SIM has been removed or the MS has been switched off.

3.3.5. Repersonalization

When the HPLMN operator so desires a SIM can be repersonalized under control of the repersonalization key. The procedures between management center and SIM are identical with the prepersonalization and personalization procedures.
This is done under the responsibility of the network operator.

3.4. Information Storage Requirements

The SIM must contain information elements to support GSM network operations and GSM management operations related to the mobile subscriber authentication. The SIM may contain information elements related to the mobile subscriber, GSM services, PLMN related information (e.g. BCCH carrier information) or additional features.

3.4.1. Information connected to mobile subscriber

The SIM must contain a non volatile storage for the following information units:

1. serial number;
   this number uniquely identifies the SIM and contains information on the manufacturer, the version of the operating system, an SIM number, etc (see ISO 7812);

2. status of the SIM (blocked, unblocked);

3. service code (for instance GSM);

4. (pre)personalization data;

5. repersonalization data;

6. parameters related to the authentication algorithm (if necessary);

7. authentication key;

8. IMSI;

9. (pre)personalization and repersonalization key(s);

10. cipher key;

11. cipher key sequence number;

12. TMSI;

13. LAI;

14. other subscriber related information (for further study);

15. time related to periodic location updating;

16. update status;

17. forbidden PLMNs (list containing max 4 PLMNs);

18. subcriber access control class;

19. PIN disabling allowed/not allowed indicator;

20. PIN enabled/disabled indicator;

21. PIN;

22. PIN error counter;

23. personal unblocking key;

24. inter-PLMN roaming allowed/not allowed indicator (for further study).

All reasonable steps should be taken to prevent the outside world from reading the PIN, the parameters of the algorithm or the authentication, (re)personalization and unblocking keys. Access rights for each information unit are specified in Rec. GSM 11.11.

The following information is loaded at prepersonalization time:

1. the prepersonalization data;

2. the status of the SIM;
   the status indicates amongst others whether the SIM is personalized and blocked. Other indicators are for further study;

3. IMSI;

4. parameters of the authentication function (if necessary);

5. the authentication key;

6. PIN disabling allowed/not allowed indicator;

7. the (initial) PIN ;

8. the personal unblocking key ;

9. PIN error counter ;
this counter counts and stores the number of incorrect PIN entries and is set to zero;

10. repersonalization key;

The following information is loaded at personalization time:

1. subscriber related information;

2. personalization data (e.g. date);

3. subcriber access control class.

The following information is read and updated under the control of the ME:

1. cipher key;

2. TMSI;

3. LAI;

4. additional GSM services related information;

5. periodic location updating related time;

6. update status;

7. list of forbidden PLMNs;

8. cipher key sequence number.

3.4.2. Information connected to general features

The SIM may store all sorts of information elements related to the mobile subscriber (not mobile subscriber authentication), GSM services or to additional features. Both types of SIM may contain a non volatile storage for the mobile subscriber related information listed below. The application layer of the interface must provide the means to store:

1. short message service: ability to store a number of short messages;

2. charging information: ability to store the accumulated total of advice of charge indications;

3. abbreviated dialing: ability to store a number of abbreviated dialing codes (alphanumeric codes possible);

4. fixed number call: ability to store the indication that fixed number is involved and the numbers that are allowed to be called;

5. barring of outgoing calls;

6. preprogrammed PLMN selector;

It shall be possible to introduce new mobile subscriber related information elements in course of time.

4. SIM INTERFACES

4.1. Man-Machine Interface

This is defined in GSM 02.30.

4.2. SIM-ME Interface

An application protocol for describing the SIM-ME data exchanges in GSM operation shall be common to all kinds of removable SIM.

5. COMBINED SIMS

The possibility exists that an MS with a plug-in SIM may also have provision for accepting a IC card. In this case the IC card takes precedence over the plug-in SIM.

If the IC card is inserted during a call, the IC card will take precedence after the call has finished. If the IC card is removed then the plug-in SIM takes over the security function. If an IC card is removed during a call, the call is terminated.

ANNEX

SIM IMPLEMENTATION DEPENDENT FUNCTIONS

The protocols at the SIM-ME interface, for the layers below the application layer, may depend on the SIM implementation.

A.1. IC Card SIM

ISO standards ISO 7816/1, /2 and /3 shall apply for the SIM-ME interface.

A.2. Plug-in SIM

One type of protocol for the logical interface SIM-ME shall be standardized within GSM. It is foreseen that ISO 7816/3 will apply.