SERVICES
ISSUE: OCT 2004

GSM Subscriber Identity Module (SIM) Card (16 KB)

GENERIC REQUIREMENTS
NO. GR/SIM-02/01.OCT 2004

TELECOMMUNICATION ENGINEERING CENTRE
KHURSHID LAL BHAWAN, JANPATH
NEW DELHI - 110001
INDIA

TABLE OF CONTENTS

Telecommunication Engineering Centre
(Department of Telecom Operations)

Subscriber Identity Module (SIM) Card
(GR/SIM-02/01. OCT 2004)

1.0 Scope

This generic requirement relates to the Subscriber Identity Module (SIM) complying to GSM Phase 2/ Phase-2+ for use in Mobile Equipment (ME) to interface with India Mobile Personal Communication System (IMPCS) based on GSM technology for the Department of Telecom operations. The document covers briefly the role of SIM, its components, functions, physical & electrical characteristics, electronic signals and transmission protocols, logical model and security features.

2.0 Role of SIM

In GSM, a Mobile Station (MS) is split into two parts, one containing the hardware and software specific to the radio interface and the other containing the subscriber specific data. This later part is called SIM. A subscriber identity module is a smart card, which holds all the information required to identify a particular subscription to a mobile service.

Each GSM subscriber is issued a SIM card by the operator, which can be seen as the subscriber’s “key” to the network. The SIM is inserted into the mobile terminal and the customer goes through a secure process in order to log onto the network.

The SIM card shall be used with a GSM handset approved by TEC. It shall allow the subscriber to carry with him all the special services, features and the telephone nos. (optional).

SIM shall be either a full sized smart card with perforation to facilitate cutting to a format called " Plug in SIM".

3.0 Components

The SIM card has CPU, ROM, RAM and EPROM as integrated components. Each of these components has a specific role to play.

3.1 Central Processing Unit (CPU)

The CPU is the “intelligence” of the chip and performs all the mathematical calculations and takes all the decisions required by the SIM.

3.2 Read Only Memory (ROM)

The ROM shall have a sufficient memory to store the operating system which is the set of commands that SIM understands. It shall include the GSM specific A3, A8/ Comp 128 algorithms. The contents of the ROM shall be created as part of the silicon manufacturing process. They shall be permanent and it should not be possible to change them.

3. 3 Random Access Memory (RAM)

The RAM is an area of volatile memory and its contents are lost each time the power is turned off. It is used to store temporary system flags, to buffer incoming data and as a scratch pad for calculations. The memory of RAM shall be atleast 256 Bytes.

3. 4 Electrically Erasable Programmable ROM (EEPROM)

The EEPROM memory stores all of the application data such as the Operator specific parameters (e.g. IMSI) and the subscriber data (e.g. Abbreviated Dialing Nos.). This information is retained even after the power is turned off and can be modified or erased using specific electrical signals.

The SIM shall be programmable for the features like Abbreviated Dialing Numbers (ADNs), Short Message Service (SMS), Fixed Dialing Number (FDN) etc. The EEPROM memory of the SIM cards shall be 16KB.

4.0 FUNCTIONS OF SIM CARD

The SIM card shall be capable to perform the following functions within the GSM application:

a) Access Control
b) Customization
c) Service Personalization
d) Network Branding and Advertising
e) Value addition in operator services

4.1 Access Control to the Network

The SIM shall secure to prevent unauthorized access to the network services as per GSM TS 11.11 involving
i) Local access control
ii) Network access control

i) Local access control
In the Local access control the identity of the cardholder being an authorized user is achieved through a PIN (Personal Identity Number) checking procedure without transmission on the radio interface. The subscriber presents to the SIM (via the handset) a four to eight digit no. which is known only to the subscriber. The SIM shall check the presented value against that, held in its secure memory. If the two are the same then it is assumed that the cardholder is the valid user and handset access is allowed.

ii) Network access control
Once the subscriber has proven his identity to the card the second access control mechanism takes over. This is where the card proves to the GSM network that it is valid for use. It shall be as per the procedure defined in GSM TS 11.11.

4.2 Customization

It shall be possible to customize the SIM card for the services to be provided by DTO. SIM shall be capable of storing the following minimum inputs for customization:

- International Mobile Subscriber Identity (IMSI)
- Integrated Circuit Card Identification (ICC id)
- Subscriber Authentication Key (Ki)
- Personal Identification Number- 1 (PIN-1)
- Personal Identification Number- 2 (PIN-2)
- PIN Unblocking Key-1 (PUK-1)
- PIN Unblocking Key-2 (PUK-2)

4.3 Service Personalization

The SIM shall also act as a portable data storage device, which contains the subscriber related information such as ADN, SMS and FDN. SIM shall be able to support following:

- Electrical Personalization: To authenticate the chip, it shall load the customized executable program and initialize the data in the files.
- Geographical card Personalization: For printing cardholder related data on the card body.

4.4 Network Branding and Advertising

For the purpose of advertising and network branding of IMPCS network, it shall be possible to print artwork containing DTO logo and other network related information on SIM card with high precision and quality. It shall be possible to accommodate any change in the artwork design in the subsequent batch of SIM cards.

4.5 Value addition in operator services

The SIM card shall also be able to provide a platform based on GSM standards 11.14 for SIM Tool Kit to facilitate launching of various value added interactive services like Mobile Banking, Tele-ticketing, Over-the-air modifications, Over the air charging (OTAC) etc. as per market demand and marketing ideas. SIM Tool Kit (STK) compatibility shall be provided as an option for SIM card16K and above.

5.0 Physical and Electrical Characteristics

SIM shall support the following physical types:

- ID-1 SIM

- Plug-in SIM

The physical characteristics of both types of SIM shall be in accordance with ISO 7816-1,2 (22,23). The following additional requirements shall be applied to ensure proper operation in the GSM environment.

5.1 Format and Layout

The information on the exterior of SIM should include at least the individual account identifier and the check digit of the IC Card Identification (as per GSM TS 11.11 clause 10, EF iccid).

5.1.1 ID-1 SIM

Format and layout of the ID-1 SIM shall be in accordance with ISO 7816-1.2 (22,23)

The card shall have rectangular shape to the following dimensions complying to ISO 7810 (1) with a tolerance of ± 5%

Width of the card	:	85.60 mm
Height of the card	:	53.98 mm
Thickness of the card :	:	00.76 mm

The card shall have a polarization mark (GSM TS 02.07 (3)), which indicates how the user should insert the card into the ME.

5.1.2 Plug-in SIM

The Plug-in SIM shall have a width of 25 mm, a height of 15 mm, and thickness 00.76 mm same as ID-1 SIM and a feature for orientation.

5.2 SIM card body material

The card body shall be made of Acrylo Butadiene Nitryl Styrene (ABS) plastic material and shall be fully compliant to GSM 11.11 specifications, with quality standards stipulated by ISO.

5.3 Physical resistance of SIM Cards

5.3.1 Electrostatic overload

The chips used in SIM cards shall comply with MIL STD 883C technical specifications and shall accept Class Three electrostatic overload (threshold > 4000 volts)

5.3.2 Working temperature

The SIM cards shall be fully compliant with GSM 11.11 specifications in terms of temperature and humidity resistance. The temperature range for full operational use shall be between –25 deg C and +70 deg C with occasional peaks of up to +85 deg C (not more than 4 hours each time and not over 100 times during the life time of the card).

5.3.3 Contact lifetime

In order to ensure good mechanical protection and good electrical contact at the same time, contacts shall be protected with a layer of nickel and an overall gold layer. Lifetime of SIM cards in terms of insertion into / extraction from a mobile phone or a card reader shall be a minimum of 10,000 cycles.

5.3.4 Contact pressure

The contact pressure shall be large enough to ensure reliable and continuous contact. The radius of any curvature of the contacting elements shall be greater than or equal to 0.8 mm over the contact area. Under no circumstances, the contact force shall be greater than 0.5 N per contact.

6.0 Electronic signals and transmission protocols

Electronic signals and transmission protocols shall be in accordance with ISO/IEC 7816-3(25)

6.1 Supply Voltage

The SIM card shall be capable to operate at 3V and 5V. It shall support both 3V and 5V mobile equipment in compliance with GSM TS 11.12.

6.2 Clock

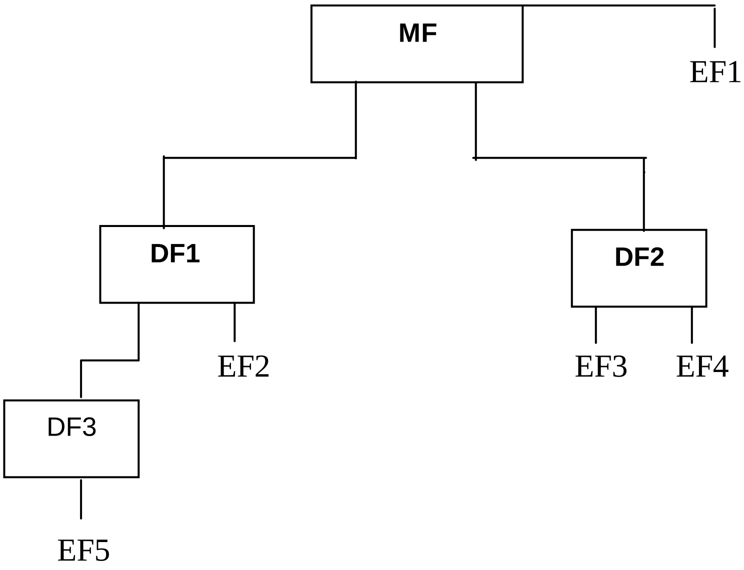
The SIM shall support clock rate 1to 5 MHz from Mobile Equipment.

6.3 Baud Rate

The Baud rate for all communication shall be: clock frequency/372.

7.0 Logical Model

The logical structure of SIM, the code associated with it and the structure of files used shall be in accordance with GSM TS 11.11 clause 6. The various files in SIM like Master file, Elementary file and dedicated files are organized in a hierarchical structure (figure 1). These files may be either administrative or application specific.



Master File (MF) : This is the unique mandatory file containing access conditions and optionally DFs and/or EFs
Dedicated File DF (DF1,DF2 ----DFn) : A dedicated file contains access conditions and , optionally, Elementary Files (EFs) or other Dedicated Files (DFs).
Elementary File EF (EF1,EF2,---EFn) : Elementary file is one which contains access conditions and data and no other file.

Figure-1

7.1 The file ID shall be assigned at the time of creation of the file concerned. No two files under the same parent shall have same ID.

7.2 All the important parameter like ICCID, IMSI, PIN, PUK etc. are stored in the EEPROM inside the SIM in the form of files. The coding and identity of the files shall be as defined in the GSM TS 11.11. Further these files are stored in directories as specified in GSM TS 11.11 as follows:

- ROOT Directory: In this directory ICCID, PIN and key files are stored.
- GSM Directory : In this directory files like IMSI Access control class, ACM, ACM max, PUCT etc. are stored
- Telecom Directory : Files like MSISDN, AND, FDN are stored in this directory

7.3 The table specifies the place of each file with respect to the directory.

Table

ROOT DIRECTORY	3F00
CHV1	0000
CHV2	0100
ADM0	1000
ADM1	1001
ADM2	1002
ADM3	1003
ADM4	1004
IccID	2FE2
EF_ICC	0002
GSM DIRECTORY	7F20
EF_Key-int	0001
EF_Key_ext	0011
SIM Service Table	6F38
IMSI	6F07
Location information	6F7E
Kc	6F20
Broadcast control channels	6F74
Access Control Class	6F78
Forbidden PLMN	6F7B
HPLMN search period	6F31
Phase identification	6FAE
Preferred Language	6F05
Administrative DF	6FAD
PLMN Selector	6F30
Cell Message Broad. Ident.	6F45
Accumulated call Meter	6F39
Advice of Charge Max	6F37
Price per Unit & Currency Table	6F41
TELECOM DIRECTORY	7F10
Short Messages Status	6F43
Short Messages Param.	6F42
Capability Configuration Param.	6F3D
MSISDN	6F40
Last Number Dialed	6F44
Extension 1	6F4A
Extension 2	6F4B
Service Dialing Number	6F49
Abbreviated Dialing Numbers	6F3A
Fixed Dialing Numbers	6F3B
Short Messages	6F3C

8.0 Security Features

Special security features in the SIM card protects data and authenticity for their entire life.

8.1 Authentication

The card security shall be based on two types of authentication

- Passive Authentication

- Active Authentication

8.1.1 Passive Authentication

Passive Authentication shall comprise of password presentation as per ISO7816-4 guidelines and verifying secret codes. The SIM card shall support seven passive authentication passwords, which consist of two user's secret code called PINs & three Administrative Secret Codes (ADM). User secret codes shall have their own unblocking secret codes called PUK (PIN unblocking key) as per GSM standards. Passwords will be initialized at the SIM vendor’s personalization center according to operator’s needs. Access conditions, which define type of authentication conditions, required to access various files use passive authentication.

8.1.1.1 Transportation password generation:

The transport of output files (which contains Ki, IMSI, ICC-id etc.) from SIM vendor to operator shall be protected by transport keys, as finalized mutually between the operator & the SIM vendor.

8.1.2 Active Authentication

Active Authentication shall comprise of Key presentation as per ISO7816-4 guidelines. It shall provide total transparent means for verification that both the card and the network have the same secret key. There shall be two types of active authentication

- Internal authentication which verify the genuineness of the card registered in the network
- External authentication ensures that an application has the right of access to certain highly sensitive files.

8.2 Network Security

The SIM card shall provide features required for authenticating itself to the GSM network and generating the keys used to cipher the calls. These features should comprise of certain keys and algorithms as per the procedure at 4.1 (ii)

8.2.1 Algorithms and processes

Following algorithms shall be supported by the SIM:

Algorithm A3 to authenticate the MS to the network	Comp 128
Algorithm A8 to generate the encryption key	

These algorithms may exist either discretely or combined (into Comp 128) with in the SIM. In either case the output on the SIM-ME interface shall be 12 bytes. The inputs to both A3 and A8, or Comp 128 are Ki (128 bits) internally derived in the SIM, and RAND across the SIM/ME interface. The output shall be SRES (32 bits)/Kc (64 bits) the coding of which is defined in the command RUN GSM ALGORITHM in clause 9 of GSM 11.11

8.3 Additional security features

Following additional security features that shall be available in the SIM card are described below:

- Additional Elementary files (EF) created inside the card shall be managed as per GSM 11.11 recommendations. As security policy depends on GSM operator needs, three states shall be made available for accessing data from the external world:
    - Under no condition
    - Under secret code control (PIN code, or administrative secret code)
    - Never (EF locked)

- Unique serial number to avoid card cloning

- “Inhibition systems” to prevent any power value out of range of the specification: Clock frequency, power supply value.

- Manufacturing diversified secret code to be presented before any EEPROM allocation.

- Read/Update access to EEPROM 100% controlled by ROM software and issuer application.

8.4 Anti tear mechanism

Card shall have **anti tear mechanism** to prevent SIM data damage during accidental voltage cut off (battery failures, battery pull out without switch off etc.)

Annex 1

Definitions

For the purposes of this document, the following definitions apply. For further information and definitions refer to GSM 01.02 [1].

Access conditions: A set of security attributes associated with a file.
Application: An application consists of a set of security mechanisms, files, data and protocols (excluding transmission protocols).
Application protocol: The set of procedures required by the application.
Card session: A link between the card and the external world starting with the ATR and ending with a subsequent reset or a deactivation of the card.
Current directory: The latest MF or DF selected.
Current EF: The latest EF selected.
Data field: Obsolete term for Elementary File.
Dedicated File (DF): A file containing access conditions and, optionally, Elementary Files (EFs) or other Dedicated Files (DFs).
Elementary File (EF): A file containing access conditions and data and no other files.
File identifier: The 2 bytes which address a file in the SIM.
GSM or DCS 1800 application: Set of security mechanisms, files, data and protocols required by GSM or DCS 1800.
GSM session: That part of the card session dedicated to the GSM operation.
IC card SIM: Obsolete term for ID-1 SIM.
ID-1 SIM: The SIM having the format of an ID-1 card (see ISO 7816-1 [24]).
Master File (MF): The unique mandatory file containing access conditions and optionally DFs and/or EFs.
Padding: One or more bits appended to a message in order to cause the message to contain the required number of bits or bytes.
Plug-in SIM: A Second format of SIM (specified in clause 2.0).
Record: A string of bytes within an EF handled as a single entity (see clause 6).
Record number: The number which identifies a record within an EF.
Record pointer: The pointer which addresses one record in an EF.
SIM application toolkit procedures: Defined in GSM 11.14 [27].

Annex 2

Abbreviations

For the purpose of this document, the following abbreviations apply, in addition to those listed in GSM 01.04 [2]:

A3	Algorithm 3, authentication algorithm; used for authenticating the subscriber
A5	Algorithm 5, cipher algorithm; used for enciphering/deciphering data
A8	Algorithm 8, cipher key generator; used to generate K_C
A38	A single algorithm performing the functions of A3 and A8
ABS	Acrylo Butadiene Nitryl Styrene
ACM	Accumulated Call Meter
ADN	Abbreviated Dialling Number
ADM	Access condition to an EF which is under the control of the authority which creates this file
ALW	Always
AoC	Advice of Charge
ATR	Answer To Reset
BCCH	Broadcast Control Channel
BCD	Binary Coded Decimal
BDN	Barred Dialling Number
BTS	Base Transmitter Station
CB	Cell Broadcast
CBMI	Cell Broadcast Message Identifier
CCP	Capability/Configuration Parameter
CHV	Card Holder Verification information; access condition used by the SIM for the verification of the identity of the user
CLA	Class
DCS	Digital Cellular System
DF	Dedicated File (abbreviation formerly used for Data Field)
DTMF	Dual Tone Multiple Frequency
ECC	Emergency Call Code
EF	Elementary File
ETSI	European Telecommunications Standards Institute
FDN	Fixed Dialling Number
GSM	Global System for Mobile communications
HPLMN	Home PLMN
IC	Integrated Circuit
ICC	Integrated Circuit(s) Card
ID	Identifier
IEC	International Electro-technical Commission
IMSI	International Mobile Subscriber Identity
ISO	International organisation 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 Dialled
LSB	Least Significant Bit
MCC	Mobile Country Code
ME	Mobile Equipment
MF	Master File
MMI	Man Machine Interface
MNC	Mobile Network Code
MS	Mobile Station
MSISDN	Mobile Station international ISDN number
MSB	Most Significant Bit
PIN	Personal Identification Number
PLMN	Public Land Mobile Network
PUK	PIN Unblocking
RAND	A Random challenge issued by the network
SDN	Service Dialling Number
SIM	Subscriber Identity Module
SMS	Short Message Service
SRES	Signed Response calculated by a SIM
TMSI	Temporary Mobile Subscriber Identity
UNBLOCK CHV1/2	value to unblock CHV1/CHV2
VBS	Voice Broadcast Service
VGCS	Voice Group Call Service
VPLMN	Visited PLMN

Annex 3

References

[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 02.07: "Digital cellular telecommunications system (Phase 2+); Mobile Stations (MS) features".

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

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

[6] GSM 02.17: "Digital cellular telecommunications system (Phase 2+); Subscriber Identity Modules (SIM) Functional characteristics".

[7] GSM 02.24: "Digital cellular telecommunications system (Phase 2+); Description of Charge Advice Information (CAI)".

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

[9] GSM 02.86: "Digital cellular telecommunications system (Phase 2+); Advice of charge (AoC) Supplementary Services - Stage 1".

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

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

[12] GSM 03.38: "Digital cellular telecommunications system (Phase 2+); Alphabets and language-specific information".

[13] GSM 03.40: "Digital cellular telecommunications system (Phase 2+); Technical realization of the Short Message Service (SMS) Point-to-Point (PP)".

[14] GSM 03.41: "Digital cellular telecommunications system (Phase 2+); Technical realization of Short Message Service Cell Broadcast (SMSCB)".

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

[16] GSM 04.11: "Digital cellular telecommunications system (Phase 2+); Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[17] GSM 09.91 (ETR 174): "Digital cellular telecommunications system; Interworking aspects of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface between Phase 1 and Phase 2".

[18] CCITT Recommendation E.118: "The international telecommunication charge card".

[19] CCITT Recommendation E.164: "Numbering plan for the ISDN era".

[20] CCITT Recommendation T.50: "International Alphabet No. 5". (ISO 646: 1983, Information processing - ISO 7-bits coded characters set for information interchange).

[21] ISO/IEC 7810 (1995): "Identification cards - Physical characteristics".

[22] ISO/IEC 7811-1 (1995): "Identification cards - Recording technique - Part 1: Embossing".

[23] ISO/IEC 7811-3 (1995): "Identification cards - Recording technique - Part 3: Location of embossed characters on ID-1 cards".

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

[25] ISO 7816-2 (1988): "Identification cards - Integrated circuit(s) cards with contacts, Part 2: Dimensions and locations of the contacts".

[26] ISO/IEC 7816-3 (1989): "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[27] GSM 11.14 (TS 101 267): "Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface".

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

[29] GSM 02.22: "Digital cellular telecommunications system (Phase 2+); Personalization of GSM Mobile Equipment (ME) Mobile functionality specification".

[30] ISO 639 (1988): "Code for the representation of names of languages".

[31] ISO/IEC 10646-1:1993 "Information technology -- Universal Multiple-Octet Coded Character Set (UCS) -- Part 1: Architecture and Basic Multilingual Plane"

[32] GSM 03.60: "Digital cellular telecommunications system (Phase 2+); General Packet Radio service (GPRS); Service description; Stage 2"

- End of document-