ETSI TS 101 413 V7.1.0 (1999-07)

Technical Specification

Digital cellular telecommunications system (Phase 2+);
Subscriber Identity Module Application Programming Interface (SIM API);
Service description;
Stage 1
(GSM 02.19 version 7.1.0 Release 1998)

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

Reference

DTS/SMG-090219Q7 (d3003ic3.PDF)

Keywords

Digital cellular telecommunications system,
Global System for Mobile communications (GSM)

ETSI

Postal address

F-06921 Sophia Antipolis Cedex - FRANCE

Office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - 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

Internet

secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
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 SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** 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 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 Special Mobile Group (SMG).

The present document details the stage 1 aspects (overall service description) for the support of a Subscriber Identity Module Application Programming Interface (SIM API)

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 Phase 2+ Release 1998

x the second digit is incremented for 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.

1 Scope

The present document defines the stage one description of the Subscriber Identity Module Application Programming Interface (SIM API) internal to the SIM. Stage one is an overall service description, and does not deal with the implementation details of the API.

The present document includes information applicable to network operators, service providers and terminal, SIM, switch and database manufacturers.

The present document contains the core requirements which are sufficient to provide a complete service.

It is highly desirable however, that technical solutions for a SIM API should be sufficiently flexible to allow for possible enhancements. Additional functionalities not documented in the present document may implement requirements which are considered outside the scope of the present document. This additional functionality may be on a network-wide basis, nation-wide basis or particular to a group of users. Such additional functionality shall not compromise conformance to the core requirements of the service.

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

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

[3] 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".

[4] GSM 03.48: "Digital cellular telecommunications system (Phase 2+); Security Mechanisms for the SIM application toolkit; Stage 2".

[5] ISO/IEC 7816-3:1997 "Identification cards - Integrated circuit(s) cards with contacts, Part 3: Electronic signals and transmission protocols".

[6] ISO/IEC 7816-5:1994 "Identification cards - Integrated circuit(s) cards with contacts, Part 5: Numbering system and registration procedure for application identifiers".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

Applet: An Applet is an application built up using a number of modules which will run under the control of a virtual machine.

Bytecode: Machine independent code generated by a bytecode compiler and executed by a bytecode interpreter.

Data Structure: A collection of related data values such as the age, birth date and height of an individual.

Framework: A framework defines a set of Application Programming Interface (API) functions and data structures for developing applications and for providing system services to those applications.

Function: A callable and executable body of computer instructions which perform a specific computation or data processing task.

GSM applet: The GSM application conforming to GSM 11.11.

Module: A collection of functions and data structures which implement an entire application or a particular application feature or capability.

SIM API Framework: Part of the SIM responsible for the handling of applications (including triggering and loading). It also contains the library for the proactive API.

Toolkit applet: Applet loaded onto the SIM seen by the mobile as being part of the SIM Toolkit application and containing only the code necessary to run the application. These applets might be downloaded over the radio interface.

Trusted Party: A trusted party can be described as an entity trusted by the card issuer with respect to security-related services and activities.

Virtual Machine: The part of the Run-time environment responsible for interpreting the bytecode.

3.2 Abbreviations

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

AC	Application Code
AID	Applet IDentifier
APDU	Application Protocol Data Unit
API	Application Programming Interface
AVN	Applet Version Number
CA	Certification Authority
CAD	Card Acceptance Device
CHV1/2	Card Holder Verification information 1 and 2
EEPROM	Electrically Erasable and Programmable Read Only Memory
EPOS	Electronic Point of Sale
FFS	For Further Study
GPRS	General Packet Radio Service
IFD	Interface Device
IN	Intelligent Network
ME	Mobile Equipment
MExE	Mobile Station Execution Environment
MS	Mobile Station
RAM	Random Access Memory
ROM	Read Only Memory
RPC	Remote Procedure Call
SIM	Subscriber Identity Module

SE	Sending Entity
SMS-CB	Short Message Service – Cell Broadcast
SMS P-P	Short Message Service, Point to Point
TAR	Toolkit Application Reference
TLV	Tag, Length, Value
USSD	Unstructured Supplementary Services Data
WAP	Wireless Application Protocol
WTLS	WAP Transport Layer Security

Further GSM related abbreviations are given in GSM 01.04 [1].

4 Description

This document describes the high level requirements for an API for the GSM SIM. This API shall allow application programmers easy access to the functions and data described in GSM 11.11 [2] and GSM 11.14 [3], such that SIM based services can be developed and loaded onto SIMs, quickly and, if necessarily, remotely, after the card has been issued.

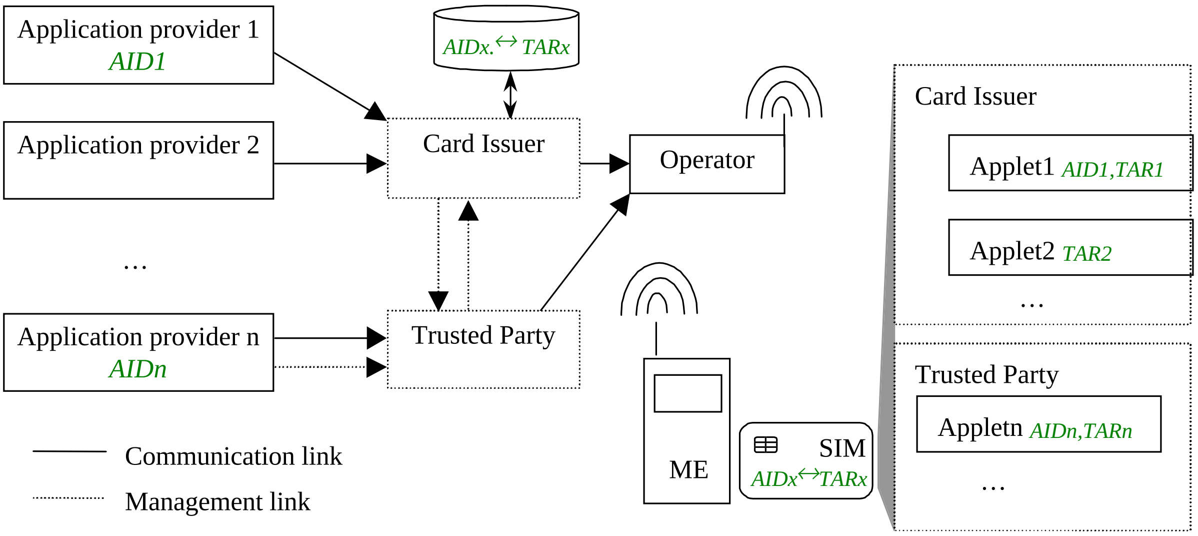


Figure 1: Toolkit applet management and communication

4.1 Design of SIM based applications using the SIM API

Figure 2 shows how SIM applications can be developed in a standard development environment and converted into an interpreted format, then loaded into the card.

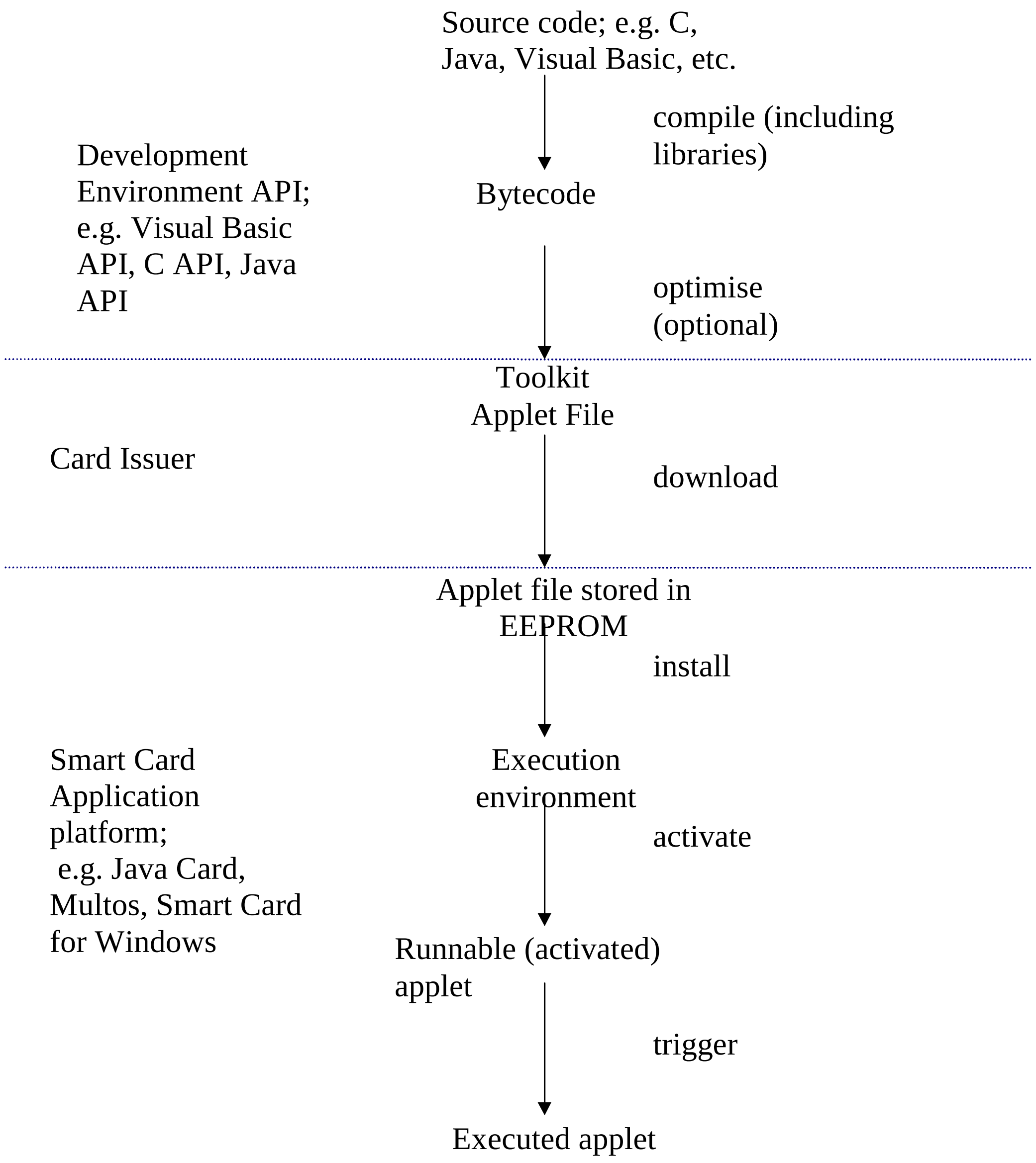
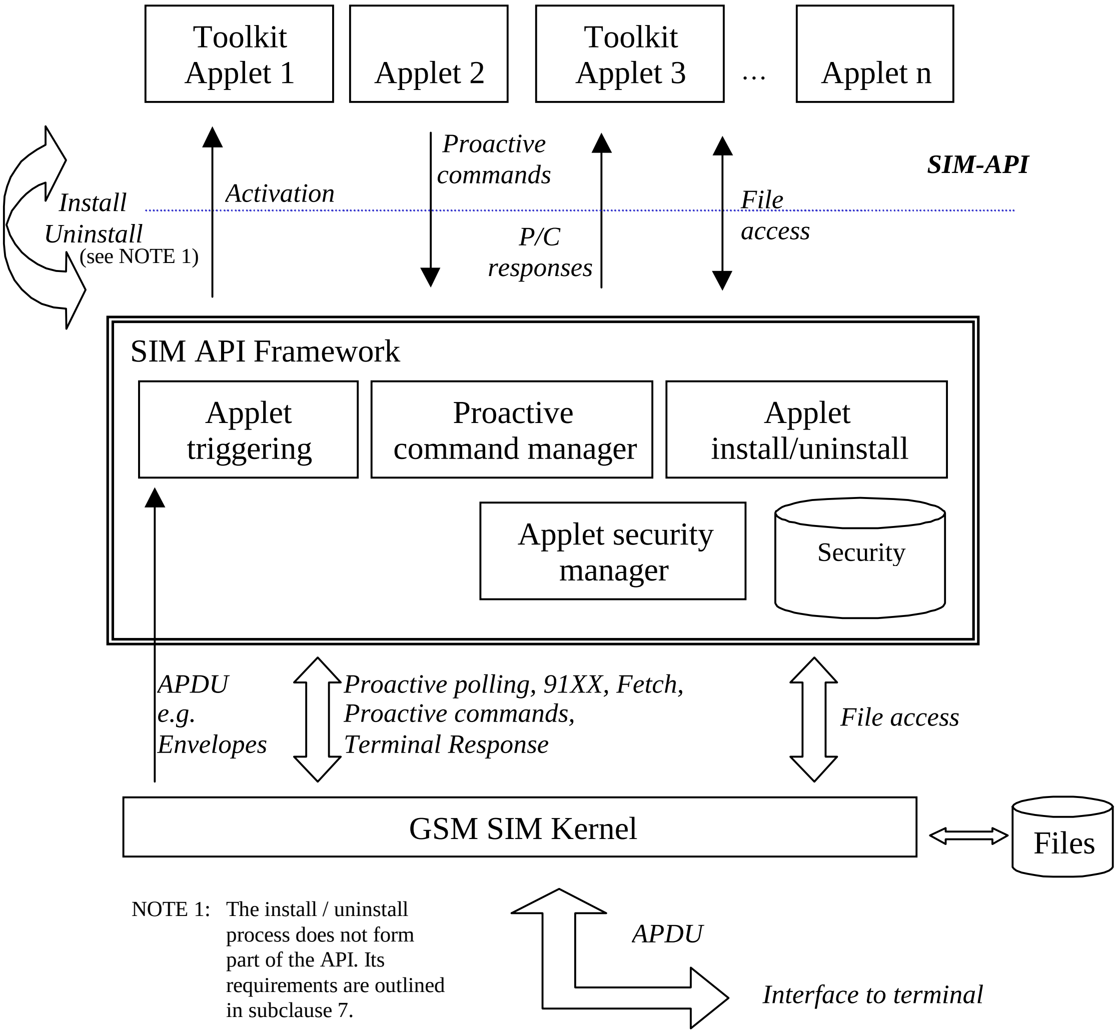

Source code; e.g. C, Java, Visual Basic, etc.
compile (including libraries)
Development Environment API; e.g. Visual Basic API, C API, Java API
Bytecode
optimise (optional)
Toolkit Applet File
Card Issuer
download
Applet file stored in EEPROM
install
Smart Card Application platform; e.g. Java Card, Multos, Smart Card for Windows
Execution environment
activate
Runnable (activated) applet
trigger
Executed applet

Figure 2: Flow diagram of the development of a SIM application

4.2 SIM API Architecture

The SIM API shall consist of APIs for GSM 11.14 [3] (pro-active functions) and GSM 11.11 [2] (transport functions). Figure 3 illustrates the interactions between these APIs.



NOTE 1: The install / uninstall process does not form part of the API. Its requirements are outlined in subclause 7.

Figure 3: SIM API Architecture

In this model, the GSM data field structure is viewed as a series of data structures and data access functions to the API. In the physical model of course, they may still be stored in elementary files, but the functions will access these data as values within those data structures.

The following figure mirrors the SIM API architecture, relating each part to the appropriate ETSI/GSM or ISO/IEC specification.

Toolkit Applet	Process (A series of instructions requiring Toolkit commands and variables)

SIM API

GSM 03.48 [4]	Transport Security Mechanisms (e.g. applied to SMS Data download)
GSM 11.14 [3]	TLVs (Built from commands and variables)
GSM 11.11 [2]	Transport of TLVs (Envelope, Fetch, Terminal Response)
	Interaction with data (Other GSM 11.11 [2] commands)

ISO/IEC 7816-3 [5]	Physical interface (e.g. T=0)

Figure 4: SIM API layers

A general requirement of the SIM API is that applets should not interfere with the basic GSM services.

4.3 GSM file data access

The following methods shall be offered by the SIM Toolkit API:

Select File: Select a file without changing the current file of any other applet or of the subscriber session. At the beginning of an entry point of an applet, the current file is the MF. This function may return the selected file information;
Status: Read the file status information of the current DF;
Read Binary: Read data bytes of a transparent EF;
Read Record: Read data bytes of a linear fixed or cyclic EF without changing the current record pointer of any other applet / subscriber. This function may allow reading part of a record;
Update Binary: Modify data bytes to a transparent EF;
Update Record: Modify data bytes to a linear fixed or cyclic EF. The current record pointer of other applets / subscriber shall not be changed in case of linear fixed EF but the current record of a cyclic EF shall be changed for all other applets / subscriber. This function may allow updating part of a record;
Seek: Search a record of a linear fixed file starting with a given pattern. The current record pointer of any other applet or of the subscriber session shall not be changed;
Increase: Increase the value of the current record of a cyclic EF. The current record will be changed for every other applet and subscriber session. This function may not return the increased value;
Rehabilitate: Rehabilitate the current EF with effect for all other applets / subscriber;
Invalidate: Invalidate the current EF with effect for all other applets / subscriber.

5 Card Interoperability

5.1 Loader Requirements

There are a number of requirements for the loader which are seen as being vital to the successful deployment of SIM API based SIMs

- The Applet format shall be common to all compliant SIMs, such that a card issuer can deploy SIM API based service applets to any SIM API compliant SIM.
- The loader environment that allows the loading of applets to the SIM shall be common to all SIM API compliant SIMs. This loader shall be able to send applets to SIMs in three distinct ways:
    - During the personalization of the SIM, prior to the issue of the SIM to the user.
    - During the life of the SIM using the SIM Data Download mechanism defined in GSM 11.11 [2] and GSM 03.48 [4] or using other standardized mechanisms in the future.
    - During the life of the SIM using an IFD (Interface Device) or CAD (Card Accepting Device, e.g. an EPOS terminal).

5.2 Application Transport

The transport of applications shall be transparent to the ME. Applications may be transported via several different bearers, e.g. SMS P-P, SMS-CB, USSD, GPRS etc. Transportation of applications to the SIM in a Phase 2+ SIM Application ME shall use the ENVELOPE command as specified in GSM 11.11 [2].

Other standardized transport commands to the SIM may be developed in the future. Transport commands other than ENVELOPE may be used to transport applets to the SIM if the SIM is not in an ME.

6 Applet triggering

The application triggering portion of the SIM API Framework is responsible for the activation of applets, based on the APDU received by the GSM application. The inputs and outputs could be represented in the figure below :

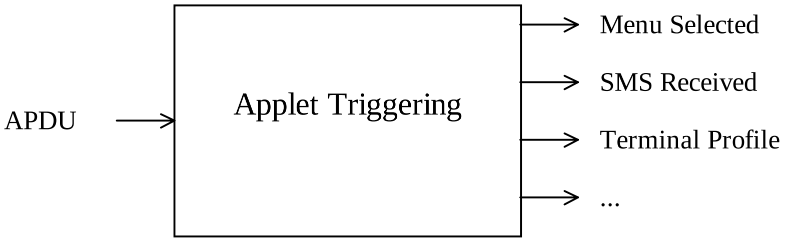


Figure 5: Applet Triggering module

Entry points to the applet shall be provided in two ways:

- High level entry points, in order to have a simple programming of the SIM card
- Low level entry points to support the evolution of the GSM 11.14 [3] specification (see Section 10.2)

Some of the high level entry points are listed below:

- Application Loading
- Application Removal
- Terminal Profile
- Menu Selection
- Short Message Reception
- Cell Broadcast Short Message Reception
- Call Control

7 Applet Life cycle management

The applet life cycle management concerns the applet preparation, loading, installation, registration, configuration, execution and removal/deactivation.

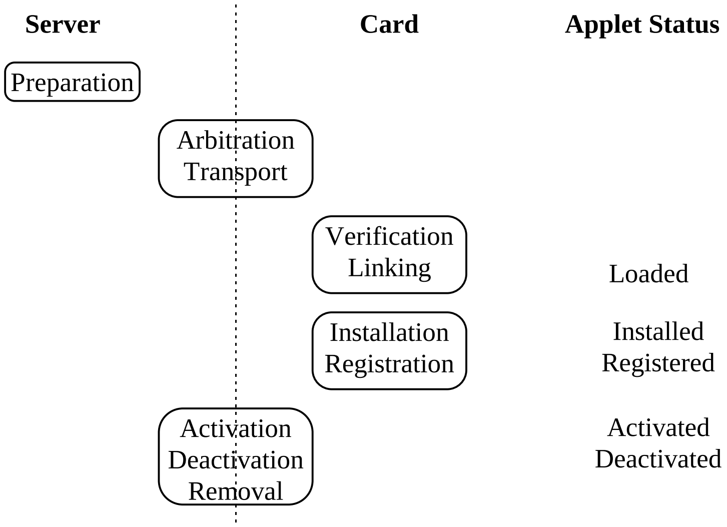


Figure 6: Applet Life Cycle

7.1 Applet Preparation

"Applet Preparation" refers to the optional phase of verifying the compliance of the applet code with card issuer standards.

The applet is to be identified through an Applet Identification Number (AID) which is assigned through the procedure detailed in ISO/IEC 7816-5 [6] and an Applet Version Number (AVN). Both AID and AVN are assigned during the applet preparation phase.

The minimum requirements for the applet (such as API versions, SIM capabilities, resource requirements) shall be specified.

7.2 Loading

"Loading" refers to the process of transporting the applet code from a load server to the SIM and generating the loaded code on the SIM.

The process shall be under the principle control of the card issuer, who may choose to delegate this responsibility to one or more trusted parties, possibly while imposing resource restrictions (e.g. maximum memory allowance) or access restrictions (e.g. limited or reduced functionality).

The loading process involves four distinct phases: Arbitration, Transport, Verification and Linking. The card shall provide acknowledgement of success or failure (including error identification code) to the load server if the load server requires this.

7.2.1 Arbitration

This phase is accomplished by mutual authentication between the SIM and the load server, and by establishing appropriate session keys for ensuring security during the data transfer, which is to follow.

The minimum applet requirements are verified with regard to the environment present on the SIM (e.g. API version, SIM capabilities and available memory). If this fails, the loading process shall be aborted.

The applet identifiers (AIDs) and version numbers (AVNs) of any applets already installed on the SIM are compared to the AID and AVN of the applet, which is to be downloaded. If an identical applet is already installed on the SIM (i.e. both applet identifier and version number match), the phases Transport, Verification and Linking are skipped. If an applet with an identical applet identifier (AID) but different version number (AVN) is available on the SIM, that applet is removed (see subclause 7.7, Removal).

7.2.2 Transport

This stage shall encompass the transport of the data packets from the load server to the SIM, and may be done in accordance with GSM 03.48 [4] and optionally additional encryption using session keys generated/exchanged during the Arbitration phase.

7.2.3 Verification

This stage shall encompass the verification of the received data and may involved byte-code level or applet-specific verification. Should the verification stage fail, the applet shall be discarded.

7.2.4 Linking

This stage shall encompass the linking of the received code against the runtime environment present on the card.

7.3 Installation/Registration/Reactivation

This stage refers to the execution of applet-code regarding to the installation and registration of the applet with respect to the SIM/ME runtime environment. For example, this may involve the generation of an applet-specific menu entry in the ME's user interface through the appropriate SIM toolkit command, and the generation of applet-specific data structures in SIM memory.

If the applet already exists on the SIM and is deactivated (see subclause 7.6), the installation request shall reactivate the applet. Other methods of reactivation are possible via a separate command.

7.4 Configuration

This stage may involve any necessary configuration of the applet code with regard to a particular user/set-up/environment. This stage is driven through code provided with the applet itself and may be executed repeatedly.

7.5 Execution

At this stage, providing the applet is activated, the applet is in a state where its execution may be triggered by any event as specified in clause 6.

7.6 Deactivation

This stage involves disabling the ability to execute applet code in the SIM and may be triggered by the user, the network operator or any third party, providing sufficient access rights are granted to them. Deactivation may include the release of any applet reserved resources (e.g. memory resources etc.).

7.7 Removal

This stage follows the deactivation of the applet and prevents the applet's reactivation. This may be followed by the release of the applet's memory. For security reasons, the memory may be overwritten by null data.

8 Security management

8.1 Management of Applets

Security might be required during the loading of the applet from a load server onto the SIM, and the communications between the applet and any remote server during the execution of the applet code. In both cases security may involve the authentication of the communicating entities and the encryption of the data traffic between those entities.

A hierarchy of keys may be bootstrapped by initializing a set of keys by the card issuer during card personalization. Additional keys may be generated, distributed using existing keys, and equipped with limited authority. Such keys may be passed on to trusted parties and subsequently used for authentication and encryption.

8.2 Applet Certification

The role of certification is to ensure that only the authorized entities are able to download an application on to the SIM. Based on this certificate, the card shall decide whether or not to accept the downloaded application.

9 API Compatibility

9.1 Level of Compatibility

The commands and features supported by the API shall be as specified in the same Release year of GSM 11.11[2] and GSM 11.14[3].

9.2 Compatibility at the Interface

In order to provide compatibility with the SIM/ME interface, a GSM application SIM implemented using the SIM API shall provide full functional compatibility with the structure and content of GSM 11.11 [2], GSM 11.14 [3] commands as specified in those documents. SIM implementing the API shall be compatible with all phases of MEs.

9.3 Compatibility at the programming interface

All commands (at the functional level) shall be presented in a manner consistent with the customary or recommended use of the programming language at the programming level.

The SIM API shall be provided in two ways:

- an easy to use high level interface (proactive commands level), and
- a low level interface (i.e. the TLV parameters) to maximise scope without the need to extend the SIM API.

9.4 Compatibility with other specifications

[TBD e.g. MExE and WAP]

10 API Extensibility

The SIM API shall support applications written for previous versions of the SIM API.

There shall be means to manage versions of the SIM API.

At installation of an applet the required SIM API version shall be checked as described in clause 7.

The ability to extend the SIM API to add functionality may be possible without reissuing the card.

10.1 Evolution of SIM / ME Interface (GSM 11.11)

As the SIM/ME interface is handled by the GSM SIM kernel any evolution of the interface may require the introduction of a new SIM API version.

Older version of the SIM API would still be allowable, but would not have access to the interface enhancement.

10.2 Evolution of SIM Application Toolkit (GSM 11.14)

The SIM API shall provide a low-level interface to support any further releases of GSM 11.14[3].

A new version of the SIM API shall provide support for the new features at a high level interface.

10.3 Interworking with other systems

If interworking at APDU and SIM API level with other systems (e.g. MExE, WAP) require some specific functionality, it will first need to be defined either in the GSM 11.11 [2] or GSM 11.14 [3], and as a result it will be taken into account in the API specification.

[Administrative command support is currently under discussion within ETSI SMG9]

11 Data and Function Sharing and Access Control

11.1 Sharing resources between applets

The API shall provide a secure data structure and function sharing mechanism between applets and with the GSM SIM kernel.

The GSM SIM kernel should be able to share with applets:

- GSM files : to get file status, read and update data field
- CHV1,CHV2 : to get status.

A toolkit applet shall be able to share any kind of data with any other applet even a non-toolkit applet.

The data and function sharing mechanism and the access control management shall be common to all card issuers.

To ease the deployment, these requirements have the following priorities:

- high: GSM SIM kernel data sharing (e.g. access to the Telecom directory),
- medium: inter industry sharing mechanism between applets.

11.2 Access to data

The SIM API shall provide a way to let each applet indicate:

- the shared data and functions,
- the associated access functions to these data and functions,
- the security or trust level required,
- the accepted certification authorities, and,
- the identity of the applet provider.

The SIM API framework shall check all these parameters before granting an access to data.

12 Technology Considerations

12.1 SIM hardware requirements

The SIM API requires a smart card device that is capable of implementing a virtual machine and the SIM API framework. It is seen as necessary that there is sufficient EEPROM to contain SIM Applets (either SIM toolkit applications or other SIM applications) along side the mandatory GSM files and potentially many (if not all) of the optional GSM files. The hardware requirements are likely to be:

- ROM:	minimum 24K Bytes
- RAM:	minimum 1K Byte
- EEPROM:	minimum 16K Bytes

12.2 Technology limitations

12.2.1 Memory Recovery

Although there is a requirement for SIM API compliant devices to allow reconfiguration, termination and removal of Applets, it is recognised that SIM API devices may not be fully capable of reclaiming the memory freed up.

12.3 Evolution

12.3.1 Remote Procedure Call

Some current technologies that meet the needs of the SIM API are not designed to allow RPC. Future alternative technologies may be able to support this. It is seen as a future requirement of SIM API when interacting with mobile equipment technologies such as MExE and WAP that RPC is supported.

Annex A (Informative):
Change History

This annex lists all change requests approved for the present document by ETSI SMG.

SMG#	SMG tdoc	SMG9 tdoc	VERS	CR	RV	PH	CAT	SUBJECT	Resulting Version
s27	98-0674	98p353	2.0.0					Approved at SMG #27	7.0.0
s29	P-99-410	9-99-203	7.0.0	A001		R98	F	Technology neutrality and implementation independence of specification	7.1.0

History

Document history		
V7.1.0	July 1999	Publication

ISBN 2-7437-3258-X
Dépôt légal : Juillet 1999