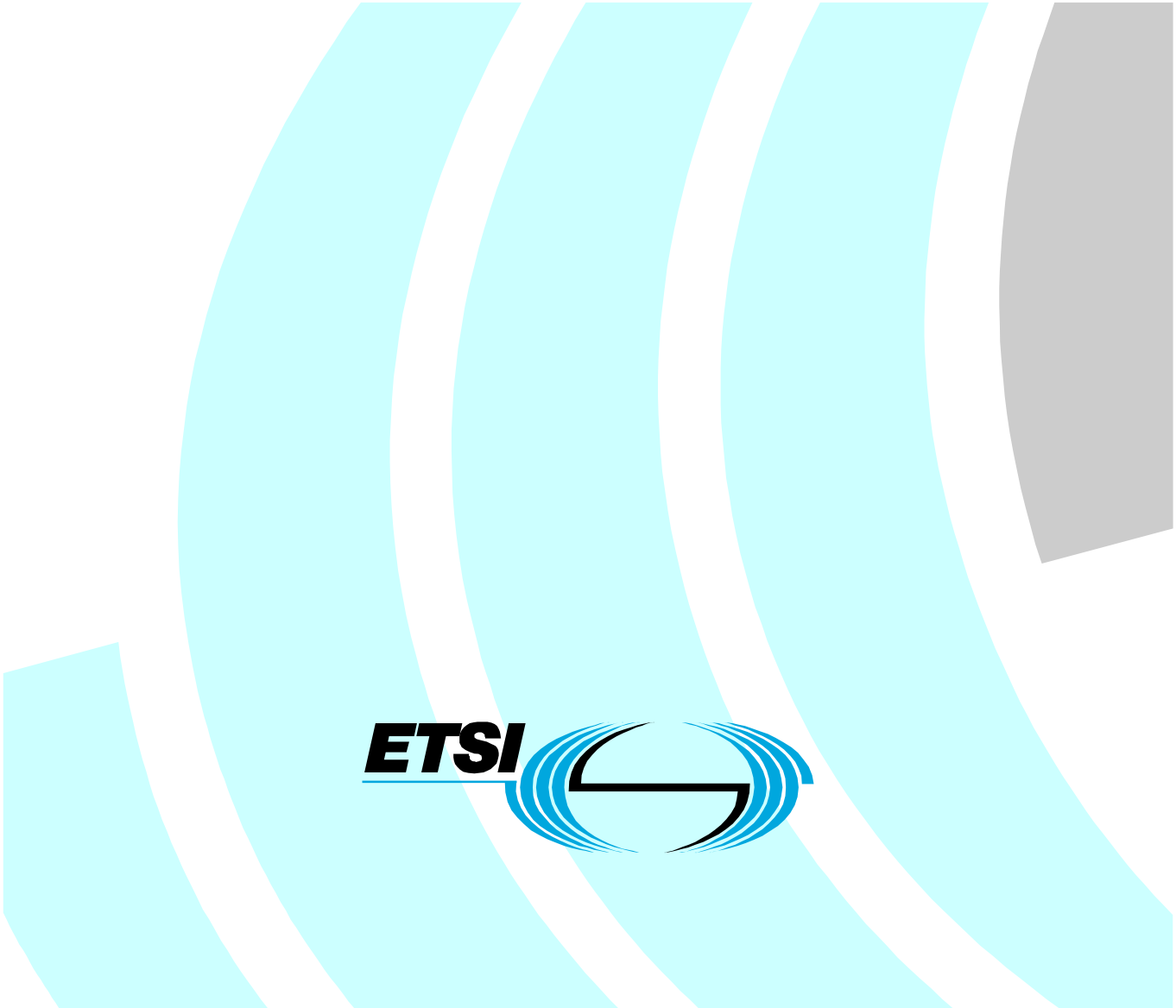
ETSI TS 102 240 V6.1.0 (2004-12)

Technical Specification

Smart Cards;
UICC Application Programming Interface and Loader Requirements;
Service description;
(Release 6)



Reference
RTS/SCP-R0263r1

Keywords
API, smart card

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

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 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://webapp.etsi.org/IPR/home.asp).

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 ETSI Project Smart Card Platform (SCP).

It is based on work originally done by the 3GPP group in "TSG-Terminals WG3" and by "ETSI Special Mobile Group (SMG)".

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

The contents of the present document are subject to continuing work within ETSI SCP and may change following formal ETSI SCP approval. Should ETSI SCP 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 x.y.z

where:

x the first digit:

0 early working draft;

1 presented to EP SCP for information;

2 presented to EP SCP for approval;

3 or greater indicates EP SCP 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 service description of the UICC Application Programming Interface (UICC API) internal to the UICC. 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, UICC, Network Access Application (NAA) providers, 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 UICC 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 and/or edition number or version number) 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 an EP SCP document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document..

[1] ETSI TS 102 221: "Smart cards; UICC-Terminal interface; Physical and logical characteristics".

[2] ETSI TS 102 223: "Smart cards; Card Application Toolkit (CAT)".

[3] 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: 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: collection of related data values such as the age, birth date and height of an individual

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

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

UICC API framework: part of the UICC responsible for the handling of applications (including triggering and loading)

NOTE: It also contains the library for the proactive API.

toolkit applet: applet loaded onto the UICC seen by the mobile as being part of the UICC toolkit application and containing only the code necessary to run the application

NOTE: These applets might be downloaded over the radio interface.

trusted party: entity trusted by the card issuer with respect to security-related services and activities

virtual machine: 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:

AID	Applet IDentifier
APDU	Application Protocol Data Unit
API	Application Programming Interface
AVN	Applet Version Number
CAD	Card Acceptance Device
CAT	Card Application Toolkit
EPOS	Electronic Point Of Sale
IFD	InterFace Device
NAA	Network Access Application
RPC	Remote Procedure Call
TLV	Tag, Length, Value
UICC	Universal Integrated Circuit Card

4 Description

The present document describes the high level requirements for an API for the UICC. This API shall allow application programmers easy access to the functions and data described in TS 102 221 [1] and TS 102 223 [2], such that UICC based services can be developed and loaded onto UICCs, quickly and, if necessarily, remotely, after the UICC has been issued.

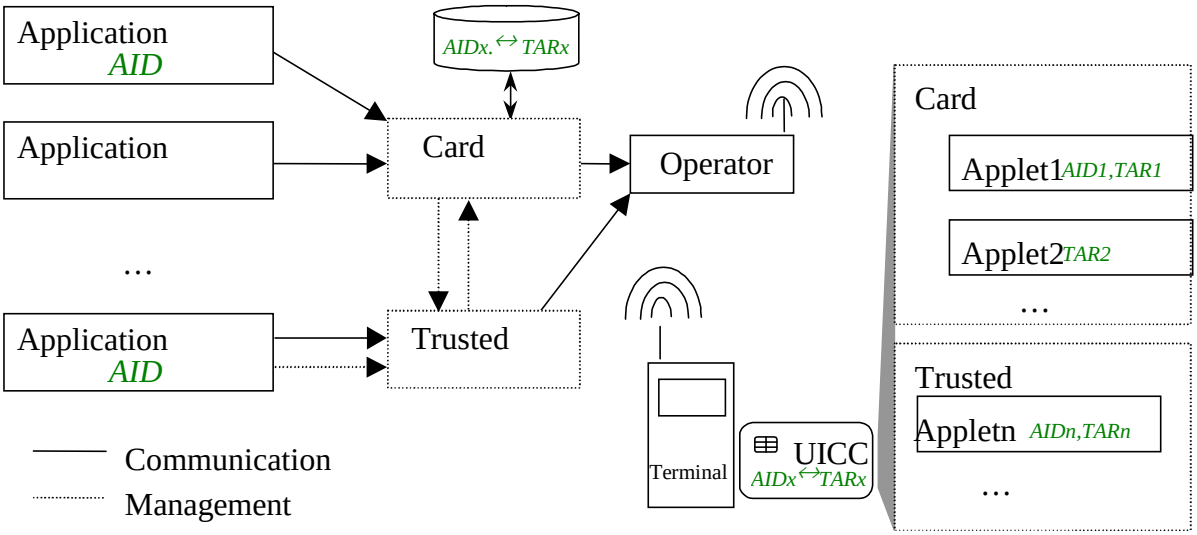


Figure 1: Toolkit applet management and communication

4.1 Design of UICC based applications using the UICC API

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

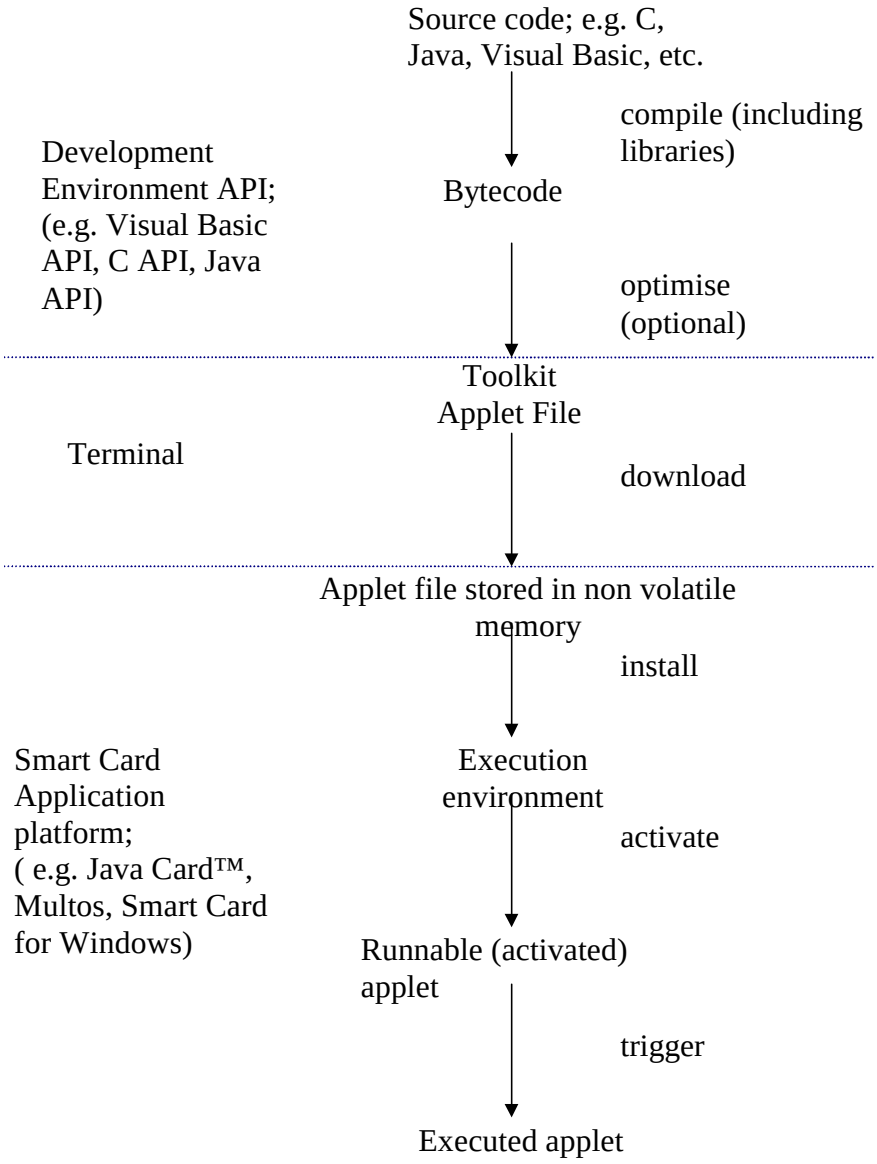


Figure 2: Flow diagram of the development of a UICC application

4.2 UICC API architecture

The UICC API shall consist of APIs for TS 102 223 [2] (pro-active functions) and TS 102 221 [1] (transport functions). Figure 3 illustrates the interactions between these APIs.

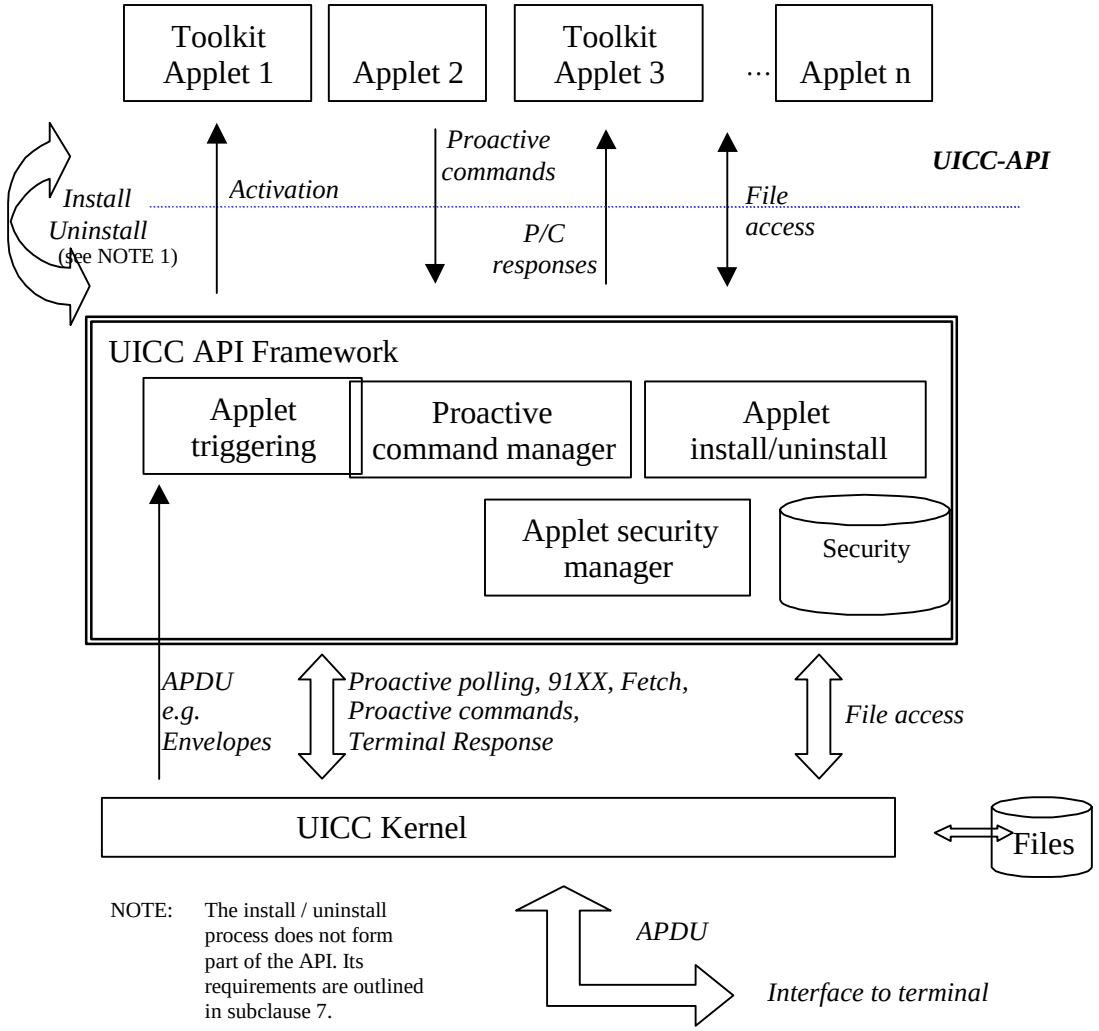


Figure 3: UICC API architecture

In this model, the UICC 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.

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

The UICC API framework shall prevent the toolkit applets from sending proactive commands which would interfere with the correct execution of the UICC operating system and/or other toolkit applets.

4.3 UICC file data access

The following methods shall be offered by the API to UICC applets, to allow access to the UICC data:

activateFile This function reactivates a deactivated EF. In case of successful execution of the command, the EF on which the command was applied becomes the current EF. After an unsuccessful execution, the current EF and current DF shall remain the same as prior to the execution.

deactivateFile	This function initiates a reversible deactivation of an EF. In case of successful execution of the command, the EF on which the command was applied becomes the current EF. After an unsuccessful execution, the current EF and current DF shall remain the same as prior to the execution.
increase	This function adds the value given in an array of bytes to the value of the last increased/updated record of the current cyclic EF, and stores the result into the oldest record. The record pointer is set to this record and this record becomes record number 1. The function does not perform the increase if the result would exceed the maximum value of the record (represented by all bytes set to "FF").
readBinary	This function reads an array of bytes from the current transparent EF.
readRecord	This function reads one complete record in the current linear fixed or cyclic EF into an array of bytes.
SearchRecord	This function searches through a linear fixed or cyclic EF to find record(s) containing a specific pattern.
select	Select a file without changing the current file of any other applet or of the subscriber session.
status	This function returns information concerning the current directory.
updateBinary	This function updates the current transparent EF with an array of bytes.
updateRecord	This function updates one specific, complete record in the current linear fixed or cyclic EF with an array of bytes.

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 UICC API based UICCs.

- The Applet format shall be common to all compliant UICCs, such that a card issuer can deploy UICC API based service applets to any UICC API compliant UICC.
- The loader environment that allows the loading of applets to the UICC shall be common to all UICC API compliant UICCs. This loader shall be able to send applets to UICCs in three distinct ways:
  - During the personalization of the UICC, prior to the issue of the UICC to the user.
  - During the life of the UICC using the UICC Data Download mechanism defined in TS 102 223 [2] or using other standardized application dependent mechanisms.
  - During the life of the UICC 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 terminal. Applications may be transported via several different bearers.

6 Applet activation

6.1 Applet triggering

The application triggering portion of the UICC Framework is responsible for the activation of toolkit applets, based on the APDU received by the UICC. The inputs and outputs could be represented in figure 4.

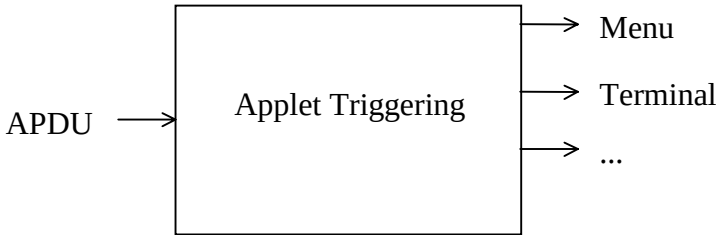


Figure 4: Applet triggering module

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

- High level entry points, in order to have a simple programming of the UICC.
- Low level entry points to support the evolution of the TS 102 223 [2] specification.

Some of the high level entry points are listed below:

- Application loading.
- Application removal.
- Terminal profile.
- Menu selection.
- …

6.2 Applet selection

Applet activation thru selection shall follow the rules defined in TS 102 221 [1] for application selection.

7 Applet life cycle management

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

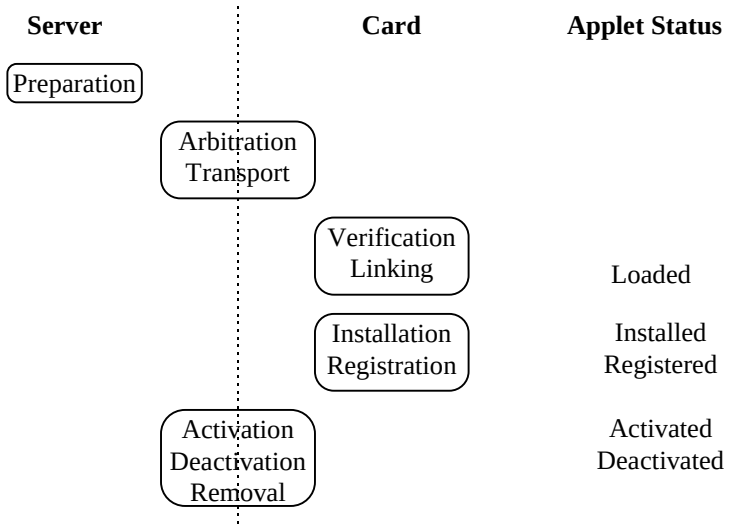


Figure 5: Applet life cycle

7.1 Applet preparation

"Applet preparation" refers to the optional phase of verifying the compliance of the applet code with card issuer or other 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 [3] 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, UICC 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 UICC and generating the loaded code on the UICC.

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 UICC 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 UICC 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 UICC (e.g. API version, UICC 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 UICC are compared to the AID and AVN of the applet, which is to be downloaded. If an identical applet is already installed on the UICC (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 UICC, that applet is removed (see clause 7.7 of the present document).

7.2.2 Transport

This stage shall encompass the transport of the data packets from the load server to the UICC, and may be done with 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 UICC.

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 UICC runtime environment and is out of scope for the present document. It may require additional procedures depending on the UICC/terminal environment (e.g. this may involve the generation of an applet-specific menu entry in the terminal's user interface through the appropriate toolkit command, and the generation of applet-specific data structures in UICC memory).

If the applet already exists on the UICC and is deactivated (see clause 7.6 of the present document), 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 of the present document.

7.6 Deactivation

This stage involves disabling the ability to execute applet code in the UICC and may be triggered by the user, the card issuer 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 UICC, 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 UICC. Based on this certificate, the UICC 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 TS 102 221 [1] and TS 102 223 [2].

9.2 Compatibility at the interface

In order to provide compatibility with the UICC/terminal interface, a UICC using the UICC API shall provide full functional compatibility with the structure and content of TS 102 221 [1] and TS 102 223 [2] commands as specified in those documents.

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 UICC 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 maximize scope without the need to extend the UICC API.

10 API extensibility

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

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

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

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

10.1 Evolution of UICC/terminal interface (TS 102 221)

As the UICC/terminal interface is handled by the UICC kernel any evolution of the interface may require the introduction of a new UICC API version.

10.2 Evolution of CAT application toolkit (TS 102 223)

The UICC API shall provide a low-level interface to support any further releases of TS 102 223 [2].

The UICC API should provide a high level interface to support specific features.

10.3 Interworking with other systems

If interworking at APDU and UICC API level with other systems (e.g. MExE, WAP) require some specific functionality, it will first need to be defined either in the TS 102 221 [1] or TS 102 223 [2], and as a result it will be taken into account in the API specification.

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 UICC kernel.

The UICC kernel should be able to share with applets:

- files: to get file status, read and update data field;
- PIN1,PIN2: 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: UICC kernel data sharing;
- medium: inter industry sharing mechanism between applets.

11.2 Access to data

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

12 Technology considerations

12.1 UICC hardware requirements

The UICC API requires a smart card device that is capable of implementing a virtual machine and the UICC API framework. It is seen as necessary that there is sufficient non volatile memory to contain UICC Applets along side mandatory application specific files and potentially many (if not all) of optional application specific files.

12.2 Technology limitations

12.2.1 Memory recovery

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

12.3 Evolution

12.3.1 Remote Procedure Call (RPC)

Some current technologies that meet the needs of the UICC API are not designed to allow RPC. Future alternative technologies may be able to support this. It is seen as a future requirement of UICC API when interacting with terminal based execution environments.

Annex A (informative): Change history

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

Date	Meeting	EP SCP Doc.	CR	Rv	Cat	Subject/Comment	Old	New
2004-11	SCP#19	N4-040456	001			Clarification for non-specific references	6.0.0	6.1.0

History

Document history		
V6.0.0	July 2002	Publication
V6.1.0	December 2004	Publication