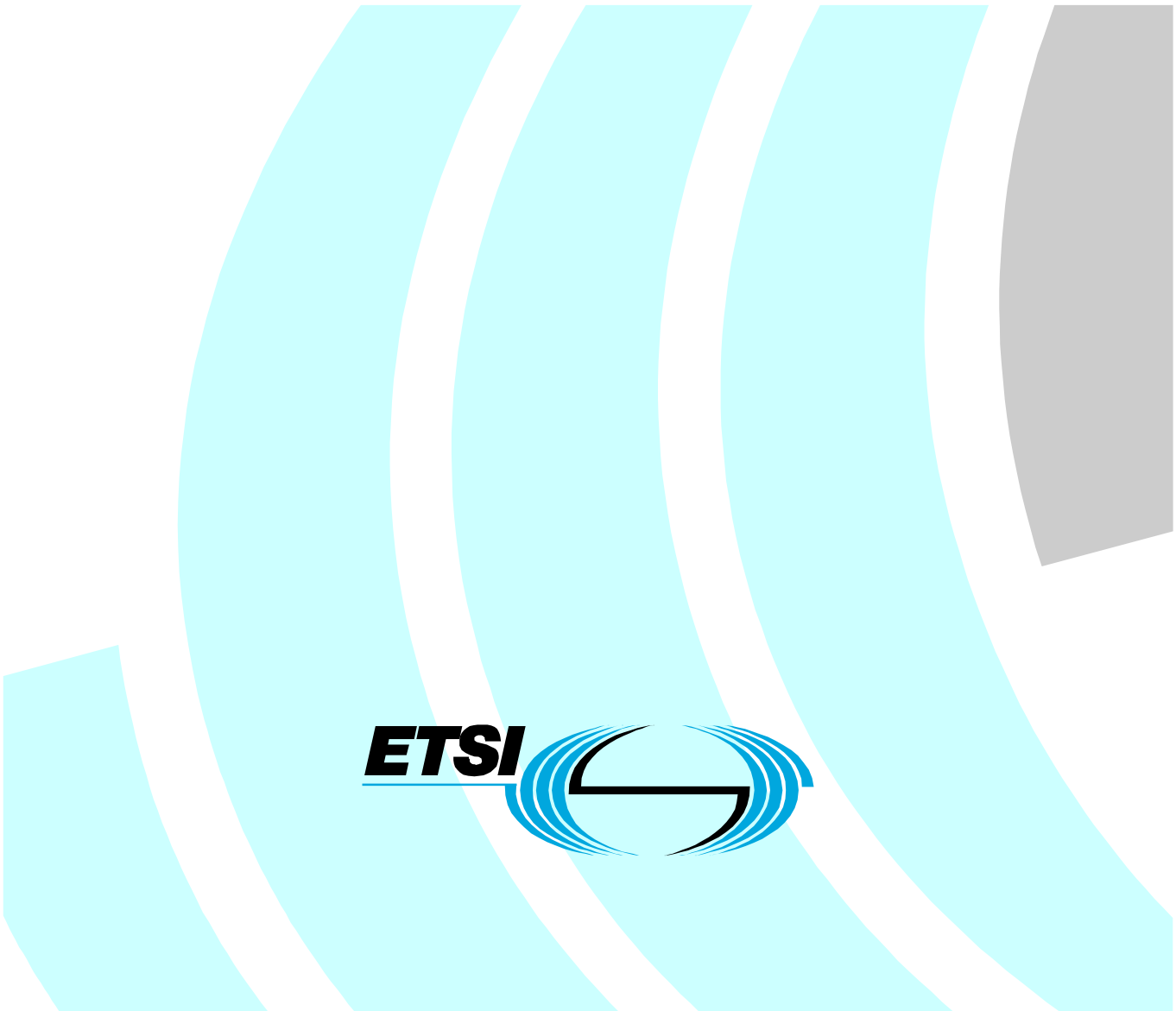
ETSI TS 102 412 V7.0.0 (2005-09)

Technical Specification

Smart cards;
Smart Card Platform Requirements
Stage 1
(Release 7)



Reference
DTS/SCP-R00002

Keywords
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).

The contents of the present document are subject to continuing work within TC SCP and may change following formal TC SCP approval. If TC SCP modifies 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 TC SCP for information;
- 2 presented to TC SCP for approval;
- 3 or greater indicates TC 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.

Introduction

The present document specifies the requirements for Release 7 of the TC SCP.

1 Scope

The present document specifies the additional requirements for Release 7 of the TC SCP with respect to earlier releases.

The present document covers all the Stage 1 requirements which are not covered by other TC SCP stage 1 documents.

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 TC SCP document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

[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) (Release 6)".

[3] 3GPP TS 22.038: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; USIM Application Toolkit (USAT); Service description; Stage 1; (Release 7)".

[4] ETSI TS 151 011: "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface (3GPP TS 51.011)".

[5] ETSI TS 131 102: "Universal Mobile Telecommunications System (UMTS); Characteristics of the USIM application (3GPP TS 31.102 Release 6)".

[6] ISO/IEC 7816-4: "Identification cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange".

3 Definitions, symbols, abbreviations and coding conventions

3.1 Definitions

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

ADF	Application Dedicated File
CAT	Card Application Toolkit
DF	Dedicated File
EF	Elementary File
IP	Internet Protocol
IMS	IP Multimedia Services
ISIM	IMS SIM
JSR	Java Specification Request
ME	Mobile Equipment
POP	Post Office Protocol
SMTP	Simple Mail Transfer Protocol
UE	User Equipment
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
WIM	Wireless Identity Module

3.4 Coding Conventions

Void.

4 Requirements

The present document specifies:

- Run time environment timing constraints;
- Launch Application command;
- Mapped file support on the UICC;
- Extension of logical channels.

4.1 Run time environment timing constraints

4.1.1 Abstract (informative)

SCP specifications up to Release 6 do not put any restrictions to the run time behaviour of smart card applications on the CAT layer and on the application layer. However, an example for a situation which requires a defined runtime behaviour of the UICC is given in a note in Release 6 of TS 102 223 [2]: The maximum work time of applications before sending a MORE TIME proactive command to the terminal should not exceed a certain amount of time. This remark is made in the context of the network authentication command and it is not normative. To avoid future problems due to this undefined behaviour, the requirements in this clause aim at providing the infrastructure needed to achieve standardized behaviour in situations like those described above from Release 7 onwards.

4.1.2 Background (informative)

4.1.2.1 Use case - Network authentication

An application may not block an UICC with a USIM application longer than a well defined period of time in order to be able to process network authentication commands within a time limit which is a network parameter (TS 102 223 [2] Release 6).

4.1.3 Requirements

REQ-7-01-01-01	The UICC shall provide a mechanism to assign a maximum work time to an application. The time value might be network specific.
REQ-7-01-01-02	The UICC shall not be blocked by an application for an amount of time exceeding the configured maximum work time.
REQ-7-01-01-03	In addition, the application itself shall be able to assign its own maximum work time value.
REQ-7-01-01-04	The application shall be suspended by the run time environment after the work time has expired and control shall be given back to run time environment.
REQ-7-01-01-05	The run time environment shall return control to the application if no other task with higher priority (e.g. network authentication) is pending.
REQ-7-01-01-06	The task switch procedure shall be transparent to the application.
REQ-7-01-01-07	Any security related to the tasks shall not be weakened by the task switch.

4.1.4 Interaction with Existing Features (informative)

(none)

4.2 Launch Application command

4.2.1 Abstract (informative)

(none)

4.2.2 Background (informative)

The present document presents a stage 1 requirement and high-level description for the Launch Application Feature.

The requirements are based on an existing requirement in the 3GPP stage 1 specification for toolkit feature 3GPP TS 22.038 release 7 [3].

As the applications to be launched are mainly independent of the air interface, it is appropriate to standardize this feature in TC-SCP rather in 3GPP. This will also make this feature available to other telecom standards.

Example of terminal applications for such a feature:

- E-mail:

CAT can launch an e-mail client on the terminal, providing parameters such as POP server, SMTP server, login, password, …

- Network management optimization:

CAT launches an application in the mobile that reports to the USIM; channels and application metrics, for network performance monitoring.

- Proactive synchronization:

CAT application, triggered by suitable events, may command the start of a data synchronization process (e.g. for subscriber related parameters or ME configuration data) that may involve data entities in the UE and in a synchronization server.

- Streaming:

CAT may launch a streaming client in the terminal to stream a video clip with the address (e.g. URL) provided by the CAT.

4.2.3 Requirements

REQ-7-02-01-01	The CAT shall be able to start a terminal application, providing its name and initial parameters.
REQ-7-02-01-02	The terminal shall inform the card (e.g. through events) about the terminal applications that can be launched by the CAT, with the corresponding information on the needed parameters to launch each terminal application.
REQ-7-02-01-03	The informing of the card shall be done after each start of card session and as soon as possible after such an eligible application is added to, or removed from the terminal.
REQ-7-02-01-04	The user of the terminal shall be able to choose when he should be prompted for the issuance of the CAT LAUNCH APPLICATION command. The prompt possibilities shall be: • The user is prompted for each application to be launched. • The user is prompted for those applications only that the user has selected, the other applications are launched without being prompted. The user is never prompted, i.e. all the applications are always launched.
REQ-7-02-01-05	Once launched, the application may interact with the user or another application, as though the user launched the application.
REQ-7-02-01-06	If the handset is not able to launch the requested application, an error mechanism shall be specified to inform the CAT, which shall include a reason code and details as to whether the error is temporary or not.
REQ-7-02-01-07	Each application shall have a unique identifier or reference.
REQ-7-02-01-08	The format of the identifier shall be standardized.
REQ-7-02-01-09	There shall be the possibility to provide the application identifier in a standardized way (SCP decides for the identifier value), or in a proprietary way (application provider decides for the identifier value).
REQ-7-02-01-10	An application parameter shall be uniquely identified.
REQ-7-02-01-11	This requirement shall be implemented as a letter class feature.

Following are additional information to enhance the general comprehension of the requirements (informative):

Depending on the terminal application A:

- The user may have a complete, partial or restricted control over the launched terminal application A. This control is not linked to the CAT capacity, but is inherent to the application A itself.

Examples of eligible applications with complete or partial user control are web browsers, email application, etc.

- Another ME application B may have a complete, partial or restricted control over the launched terminal application A. This control is not linked to the CAT capacity, but is inherent to the application A itself.

Examples of eligible applications with complete or partial control by an other ME application are synchronization application, terminal functionality tuning, etc.

4.2.4 Interaction with Existing Features (informative)

The release 7 Launch Application feature may be used to extend the LAUNCH BROWSER command in specific cases where it procures an advantage.

Other pre-release 7 features should not be impacted.

4.3 Mapped file support on the UICC

4.3.1 Abstract (informative)

(none)

4.3.2 Background (informative)

When comparing the file structure of a SIM in TS 151 011 [4] with that of a USIM in 3G TS 131 102 [5] it appears that many EFs not only have the same name and file identifier (although under different DFs) but are entirely equal by size and content parameters. This generally allows, for memory efficient implementation, to perform file mapping between SIM and USIM files as these files can be shared by both applications, i.e. necessary storage capacity is only required once.

The same is true concerning the mapping of files between multiple USIMs if the UICC is intended to be used by a single user, i.e. all user relevant files (that can be updated by the user) could be mapped.

This is why it seems necessary to standardize the mechanism to map these files.

4.3.3 Requirements

REQ-7-03-01-01	It shall be possible to map the content of EFs that are identical by type, size and content (i.e. the necessary storage capacity is only required once) at personalization or "over the air".
REQ-7-03-01-02	It shall be possible to setup a security rule to prevent a file to be mapped and thus prevent any illicit access to an existing file.
REQ-7-03-01-03	The fact that an EF is mapped with another EF shall not restrict the operations allowed on the file i.e. the file can be deleted, resized, updated, etc. EXAMPLE: File1, File2 and File3 are mapped. When File1 is updated, the content of File2 and File3 is changed accordingly. This is obvious because they share the same storage. It is possible to delete any of these 3 files in any order for example first delete File1 and after File3, the content of File2 remains unchanged.. After, when deleting the third file i.e. File2, the resources held by the file shall be released and the memory used by this file shall be set to the logical erased state
REQ-7-03-01-04	It shall be possible to have different security attributes for files that are mapped.
REQ-7-03-01-05	It shall be possible to have different life cycles for files that are mapped.

4.3.4 Interaction with Existing Features (informative)

(none)

4.4 Extension of logical channels

4.4.1 Abstract (informative)

TS 102 221 [1] currently specifies up to 3 logical channels in addition to the basic logical channel 0. It means that only four logical channels are currently specified.

4.4.2 Background (informative)

4.4.2.1 Typical problem situation

A situation can be that an UICC has an USIM application, an ISIM (or several) application, a WIM application, an application (or several) using the JSR 177 communication capabilities and a banking application, each of these applications use a different logical channel. If there are only 4 logical channels this is not possible.

In the same way a file (EF, DF, ADF) can to be accessed using different logical channels at the same time. But currently it is limited to 4 logical channel.

In the latest ISO/IEC 7816-4 [6] specification's revision, 16 additional channels has been added. This allows better flexibility when several applications run simultaneously.

4.4.2.2 Possible problem solution

The best solution is to extend the number of the logical channels, in line with ISO/IEC 7816-4 [6].

4.4.2.3 Use cases

Use case 1: JSR 177 applications

It is possible to have multiple applications running on the terminal talking to the smart card at the same time. For example multiple Java applications using JSR 177.

Use case 2: PC connection

A UICC connected to a PC may need to open multiple secured connection to different entities through different logical channels.

4.4.3 Requirements

4.4.3.1 General Requirements

REQ-7-04-01-01	An optional mechanism shall be introduced that allows to extend the number of logical channels available in addition to the basic channel (i.e. channel 0) and to the three already possible additional channels.
REQ-7-04-01-02	The mechanism introduced shall be ISO/IEC 7816-4 [6] compliant.

4.4.3.2 Backward compatibility requirements

REQ-7-04-02-01	A release 7 UICC supporting extended channels shall not prevent a pre release 7 terminal to use the release 6 logical channel functionality.
REQ-7-04-02-02	A release 7 terminal supporting extended channels shall not prevent a pre release 7 UICC to use the release 6 logical channel functionality.

4.4.4 Interaction with existing features (informative)

(none)

Annex A (informative): Change history

The table below indicates changes that have been incorporated into the present document since it was created by TC SCP.

Meeting	Plenary Tdoc	WG tdoc	VERS	CR	REV	CAT	SUBJECT	Resulting Version
SCP #19		SCPr040085					New top level requirement for UICC run time environment timing constraints	0.0.1
		SCPr040100					Addition of a Launch Application feature	
SCP #20		SCPr050050	0.0.1				Clarification of the Launch Application feature requirements	0.0.2
		SCPr050052					Mapped file support on the UICC	
SCP #21		SCPr010119	0.0.2				discussion, editorial modifications	0.0.3
	SCP-050116	SCPr050178	0.0.3				presented to SCP Plenary for information	1.0.0
		SCPr050302	1.1.0				Correction of layout as identified in SCP #21, addition of extension of logical channels	
		SCPr050343	1.1.1				Corrections of requirement numbers, addition of various abbreviations	7.0.0

History

Document history		
V7.0.0	September 2005	Publication