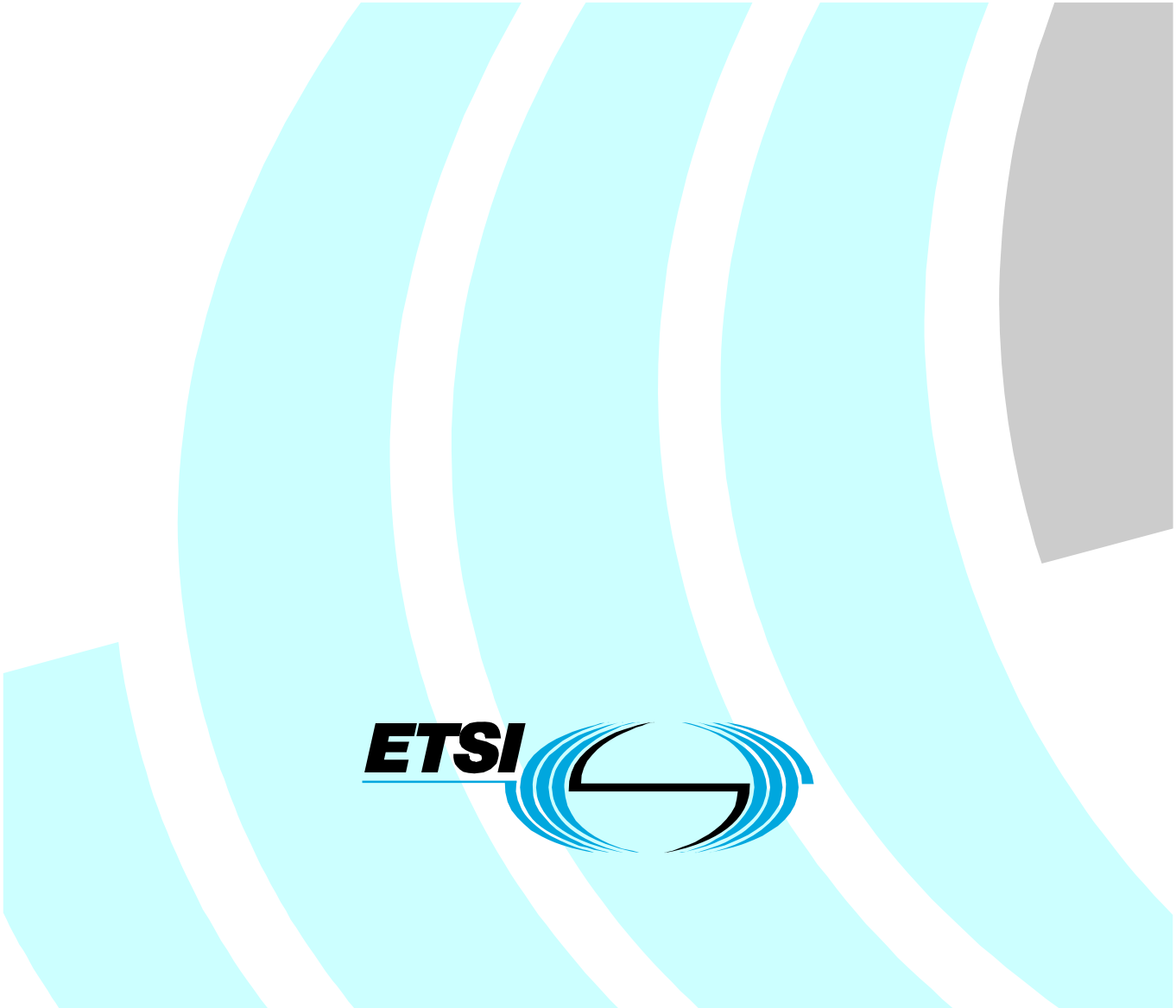
ETSI TS 102 412 V8.4.0 (2009-06)

Technical Specification

Smart Cards;
Smart Card Platform Requirements Stage 1
(Release 8)



Reference
RTS/SCP-R00002v840

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

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 Technical Committee 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 onwards of the TC SCP.

1 Scope

The present document specifies the additional requirements for Release 7 onwards 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

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.
- In the case of a reference to a TC SCP document, a non specific reference implicitly refers to the latest version of that document in the same Release as the present document.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

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

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ETSI TS 102 221: "Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 7)".

[2] ETSI TS 102 223: "Smart cards; Card Application Toolkit (CAT) (Release 6)".

[3] ETSI TS 122 038: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); USIM Application Toolkit (USAT/SAT); Service description; Stage 1 (3GPP TS 22.038 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".

[7] Trusted Computing Group (2003): "TPM Main - Part 1 Design Principles - Specification version 1.2".

NOTE: Available at http://www.trustedcomputinggroup.org/resources/tpm_main_specification_12_revision_62_parts_1__3

[8] ISO/IEC 14443 (all parts): "Identification cards - Contactless integrated circuit(s) cards - Proximity cards".

[9] ISO/IEC 18092:"Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1)".

[10] ISO/IEC 15693 (all parts): "Identification cards - Contactless integrated circuit(s) cards - Vicinity cards".

[11] ETSI EN 300 468: "Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems".

[12] ETSI EN 302 304: "Digital Video Broadcasting (DVB); Transmission System for Handheld Terminals (DVB-H)".

[13] OMA-TS-SRM-V1-0-20090310-A "OMA Secure Removable Media Specification".

[14] OMA-AD-SRM-V1-0-0-20090310-A "OMA Secure Removable Media Architecture".

[15] OMA-RD-SRM-V1-0-20090310-A "OMA Secure Removable Media Requirements".

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] GSMA Pay Buy Mobile, Business Opportunity Analysis, Public White Paper, version 1.0, November 2007.

[i.2] ISO/IEC 16750-3: "Road vehicles - Environmental conditions and testing for electrical and electronic equipment - Part 3: Mechanical loads".

[i.3] AEC-Q100: "Stress Test Qualification for Integrated Circuits".

[i.4] OMA-TS-BCAST-SvcCntProtection-V1.0 : "Service and Content Protection for Mobile Broadcast Services".

3 Definitions and abbreviations

3.1 Definitions

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

central repository: a repository of registered applications residing in the UICC

CLF: ContactLess Front-end, circuitry in the terminal which:

- Handles the analogue part of the contactless communication.
- May handle some layers of the contactless protocol.
- May exchange data with the terminal and the UICC.

CLFI (CLF Interface): physical interface between the UICC and the CLF

CLFIP (CLFI Protocol): communication protocol between the UICC and the CLF carried over the CLFI

DRM Agent: entity in the Device that manages Permissions for Media Objects on the Device, as described in OMA SRM technical specification [13]

DRM Agent-SRMAgent Mutual Authentication: DRM Agent and the SRM Agent can authenticate each other based on credentials that are securely provisioned in each. The result of this mutual authentication allows the DRM Agent and SRM Agent to establish a secure communication for the exchange and sharing of secret elements as described in the OMA SRM architecture specification [14]

HSP: high speed protocol running on top of the NUT interface

M2M communication module: electronics system including all necessary components to establish wireless communications between machines. M2M communication modules are usually integrated directly into target devices, such as automated meter readers (AMRs), vending machines, alarm systems, cars equipments or others

M2M UICC: UICC with specific properties for use in M2M environments, this includes existing form factors and an optional new form factor

Machine to Machine (Communication): communication between remotely deployed devices with specific responsibilities and requiring little or no human intervention, which are all connected to a dedicated management server via the mobile network data communications

ME/TE owner: entity having the right to configure or administrate a CAD and/or remote terminal

MFF (M2M Form Factor): a new form factor dedicated to M2M applications

Packaging: process to mount an integrated circuit device (e.g. UICC) into a package, which provides physical contacts for electric interconnection, protects the device in harsh environments and prevents the device from mechanical damage, vibration, chemistry attack and high temperatures, etc.

Rights: collection of permissions and constraints defining under which circumstances access is granted to DRM Content as described in the OMA SRM technical specification [13]

Secure Removable Media: removable media that implements means to protect against unauthorized access to its internal data and includes an SRM Agent. (e.g. secure memory card, smart card) as described in the OMA SRM technical specification [13]

Service Operator: third party that is able to manage sub-third party areas

terminal: entity with which the Smart Card can establish a secure channel

EXAMPLE 1: Card Acceptance Device such as a mobile handset i.e. in the case of a wired Smart Card to terminal (such as PDA or handset) communication.

EXAMPLE 2: A Remote Terminal is a terminal communicating to a CAD, which can access the UICC resources, for example a PC connect over a local link to handset.

NOTE: In the present document a distinction will be made between a CAD and a Remote Terminal only where applicable, in case this distinction is not relevant the generic term terminal will be used.

terminal end point: point for terminating the secure channel from the UICC point of view, which could be a Mobile Terminal or a Remote Terminal

EXAMPLE: A remote terminal can be a Set-top box, a PC, or even a Bluetooth earpiece connected to a Mobile Terminal.

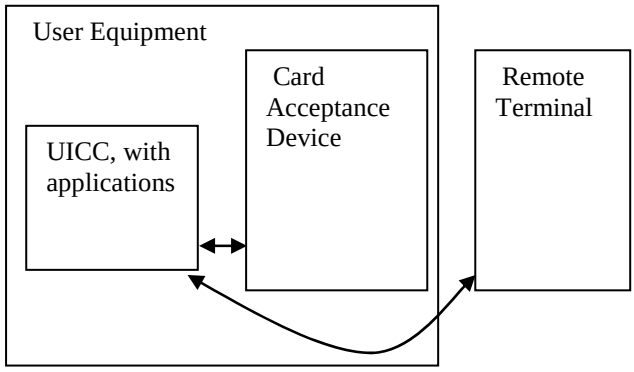


Figure 1: Possible secure channels with a UICC

third party application: application developed and installed on the card by a player different from the card issuer

third party area: area of the UICC (memory and resources) allocated to accommodate one (or several) third party application

third party policy: set of policies which define some characteristics and restrictions for the third party applications allocated into the corresponding third party areas

trusted device: device which is not infected by malevolent code, whether because it is compliant to the requirements defined in TCG [7] or because the user/owner/administrator guarantees device integrity by giving verifiable evidence

NOTE: A more exact definition is out of scope of SCP.

UICC powering modes:

- Battery powered:
  - Mode where the UICC and the CLF are powered from the battery of the terminal.
- Not Battery powered:
  - Mode where the UICC and the CLF are not powered from the battery of the terminal.

3.2 Abbreviations

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

ADF	Application Dedicated File
AEC	Automotive Electronics Council
API	Application Programming Interface
CAD	Card Acceptance Device
CAS	Conditional Access System
CAT	Card Application Toolkit
CAT-TP	Card Application Toolkit - Transport Protocol
CEK	Content Encryption Key
CPU	Central Processing Unit
DF	Dedicated File
DM	Device Management
DRM	Digital Rights Management
DRM_UA	Digital Rights Management User Agent
DVB	Digital Video Broadcasting
DVB-H	DVB-Hand held

DVB-SH	Digital Video Broadcasting - Satellite services to Handhelds
DVB-T	Digital Video Broadcasting - Terrestrial
EAP	Extensible Authentication Protocol
EF	Elementary File
GPRS	General Packet Radio Service
HTTP	HyperText Transfer Protocol
HTTPS	Secure HyperText Transfer Protocol
IMS	IP Multimedia Services
IP	Internet Protocol
ISIM	IMS SIM
JSR	Java Specification Request
M2M	Machine to Machine (communication)
MBMS	Multimedia Broadcast/Multicast Service
ME	Mobile Equipment
MFF	Machine to Machine Form Factor
MNO	Mobile Network Operator
MO	(Device) Management Object
MT	Mobile Termination
MVNO	Mobile Virtual Network Operator
NUT	New UICC-Terminal
OMA	Open Mobile Alliance
OTA	Over The Air
PDA	Personal Digital Assistance
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POP	Post Office Protocol
POS	Point Of Sale
RFID	Radio Frequency Identification
RO	Rights Object
SC	Smart Card
SCWS	Smart Card Web Server
SMTP	Simple Mail Transfer Protocol
SRM	Secure Removable Media
TCG	Trusted Computing Group
T-DMB	Terrestrial - Digital Multimedia Broadcasting
TLS	Transport Layer Security
TMP	Trusted Media Player
TSM	Trusted Service Manager
UA	(Digital Rights Management) User Agent
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
USSM	UICC Security Service Module
WIM	Wireless Identity Module

4 Requirements

The present document specifies:

- run time environment timing constraints;
- launch application command;
- mapped file support on the UICC;
- extension of logical channels;
- secure channel to secure local terminal interfaces;
- authenticate command longer than 255 bytes;

- CAT mechanisms to indicate the bearer connection status;
- New UICC-Terminal (NUT) interface;
- Smart Card Web Server running in UICC;
- API for applications registered to a Smart Card Web Server;
- specific UICC environmental conditions;
- introduction of high density memory technology in UICC;
- power supply indication mechanism;
- Internet Connectivity up to UICC applications;
- contactless UICC services;
- administration of the Smart Card Web Server;
- confidential application services;
- UICC for Machine-to-Machine (M2M) applications;
- Location based services for broadcast technology;
- terminals with reduced functionality;
- OMA Secure Removable Media capability for the UICC.

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 a 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]).

4.1.3 Requirements

Identifier	Requirement
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 feature

4.2.1 Abstract (informative)

This feature enables the UICC to discover, launch and communicate with an application on a terminal using proactive commands.

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 TS 122 038 [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, etc.

- 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

Identifier	Requirement
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.
REQ-7-02-01-12	The UICC shall have proactive mechanisms that allow it to communicate with an application it has launched.
REQ-7-02-01-13	Closing the communication with a launched application shall not automatically end the launched terminal application.

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 another 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 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

Identifier	Requirement
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 from being 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 a 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 be accessed using different logical channels at the same time, currently it is limited to 4 logical channels.

In the latest ISO/IEC 7816-4 [6] specification's revision, 16 additional channels have 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

4.4.2.3.1 Use case - 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.

4.4.2.3.2 Use case - PC connection

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

4.4.3 Requirements

4.4.3.1 General requirements

Identifier	Requirement
REQ-7-04-01-01	An optional mechanism shall be introduced that allows the extension of 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

Identifier	Requirement
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).

4.5 Secure channel to secure local terminal interfaces

4.5.1 Abstract (informative)

This clause defines requirements for a generic solution of a secure channel between the UICC and an end point terminal. Several applications will be able to rely on this generic solution to offer an end to end security.

- Providing mutual authentication between a UICC and a terminal end point.
- Providing integrity and confidentiality (encryption) protection of the interface between a UICC and a terminal end point.

The use cases in this clause will justify the need of a secure channel between a UICC and a terminal; it also lists the requirements that this secure channel shall fulfil to address all the use cases described herein.

Standardization efforts have been undergone and are at present being made to define secure channels between communicating applications running on distant platforms.

4.5.2 Background (informative)

System security can be obtained only if end-to-end protection is achieved. For Smart Card to terminal communication, this involves:

- Secure end on the Smart Card side. This is true by assumption; the Smart Card is a tamper resistant device.
- Secure end on the terminal side. This is attainable when trusted devices are employed. For example TCG [7] is specifying trusted device features and architectures.
- Secure communication between end devices, that is, the Smart Card and the terminal.

Multiple scenarios exist in which a secure communication between Smart Card and terminal is necessary. Smart cards are resource-limited devices, whose main purpose is to safeguard user identities and secret keys, and to perform sensitive cryptographic computations. Smart card use greatly depends on the environment in which they are deployed. For example, in banking, user information includes identity, account information, and possibly information on the latest transactions made and secret keys used in security functions. The operations allowed encompass card holder authentication, automatic transaction registration, transaction non-repudiation. In mobile communications, user information includes identity, personal information such as address book, operator related information, and again secret keys used in security functions. Functions executed comprehend user authentication, voice encryption, as well as data access to user's private information.

Smart cards were designed to be economic, portable and therefore small and light, yet secure. There are no peripherals that allow user direct access, such as a keyboard or a screen: Smart Card access must go through a terminal, and, unless the communication is secure end-to-end, this may constitute a security weakness. System security is that of the weakest link and, unless strengthened, attackers may target the terminal or the data exchange with the terminal to get round the robustness of the tamper resistant device.

The definition and use of trusted terminals is out of the scope of this submission. In the following clauses we will assume the terminal is not infected by malevolent code, whether because it is compliant to the requirements defined in TCG [7] or because the user/owner/administrator guarantees device integrity by giving verifiable evidence.

Multiple use cases justify the need for a Smart Card to terminal secure communication. In the following parts, we cover use cases linked with User Interface, Device Management (DM), Digital Right Management (DRM).

4.5.2.1 Use case - User interface

A large amount of information currently flows in GSM/3G network-enabled services that make use of application server software and toolkit applications. In most of these services, at least a part of the information flow has no protection from eavesdropping or tampering: if we focus on the communication between the UICC and the terminal, the information flowing from the card to the terminal, and vice versa, is in plain text [2].

In this respect, let us consider the two cases in the following:

- When an application on the UICC requires the user to enter a PIN to access a service, the PIN itself is not protected. Therefore, when PIN data is sent from the handset to the UICC, it may be stolen or maliciously altered in order to deny the service to the end user.
- When an application on the UICC sends data to the terminal to display to the user, the data is displayed in plain text. Such data may involve, for example, fees to be paid or acceptance of onerous conditions for the use of a software/service. If data is tampered with, the user may take upon him/herself a burden different from that which has been notified. Issues may be raised on how "legally binding" for a user is the acceptance of conditions that have no protection against malicious alteration before submission to the user itself.

The implementation of a secure channel will allow a secure data exchange between the end user and the service provider.

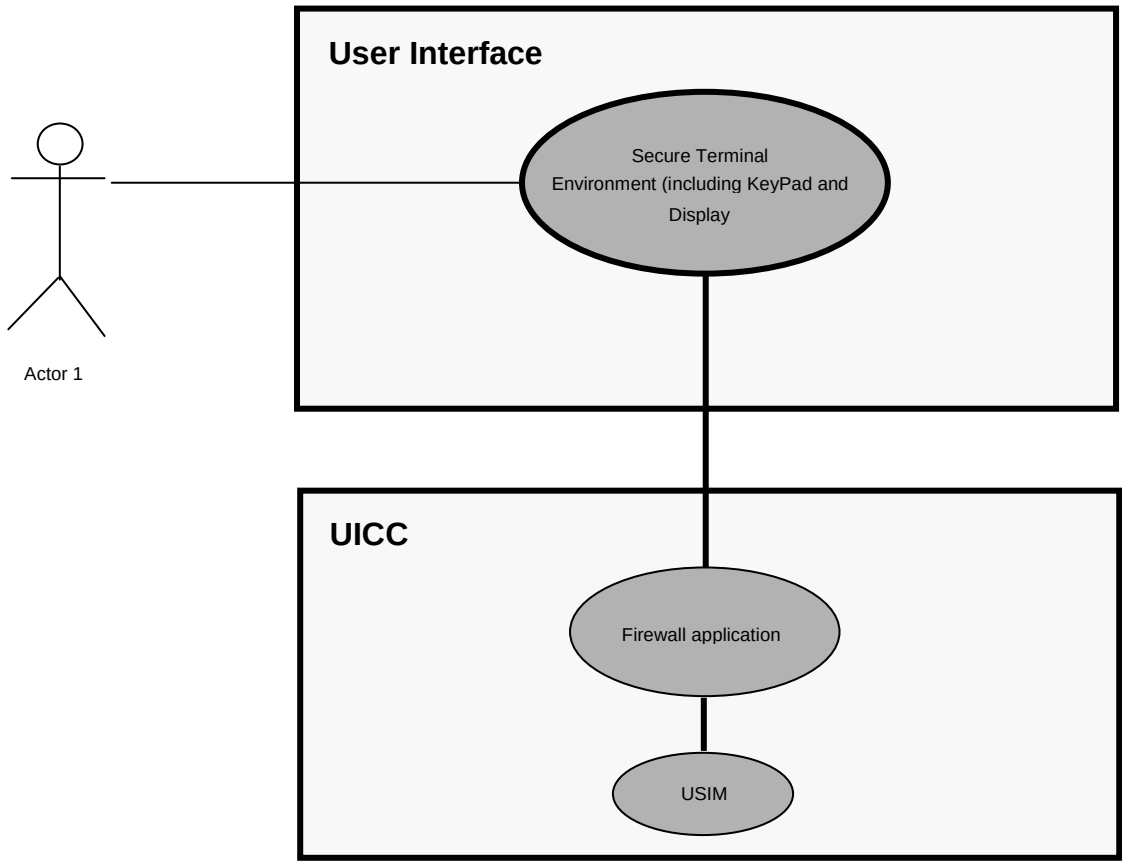


Figure 2: User Interfaces

4.5.2.2 Use case - UICC as a control point for device management

Device Management, or DM, specified in OMA, intends to provide the protocols and mechanisms allowing to remotely achieve management of devices. The Device Management includes:

- Setting initial configuration information in devices.
- Subsequent installation and updates of persistent information in devices (firmware update).
- Retrieval of management information from devices.
- Processing events and alarms generated by devices.

In this environment, the Smart Card inserted in the device is expected to play a role at least in the following cases:

- Dynamic provisioning of the device with up-to-date information.
- Handling of a part of the security during the update of device firmware (service access controlled by the operator, authentication of the origin, etc.).

It means that the Smart Card (SC) shall store DM objects (Management Objects, or MO) accessible by the device through the SC to device interface and also manageable by a remote server (through the device). This interface is currently not ciphered and DM information will be exchanged without protection. It is easy to imagine some of the possible threats occurring during these exchanges:

- When the provisioning data is extracted from the SC by the device, some man-in-the-middle application or element could intercept and change some data in order to alter the device configuration or compel the device to connect to a fraudulent DM server. The data should therefore be ciphered.

An unauthorized server or device agent could try to modify the information stored into the SC leading to a later bad provisioning of the device. Therefore, only authorized and authenticated device agents or remote servers should be able to update or modify or add DM data in the SC.

The availability of a secure channel will allow to secure and protect the communications occurring between the device DM user agent and the Smart Card.

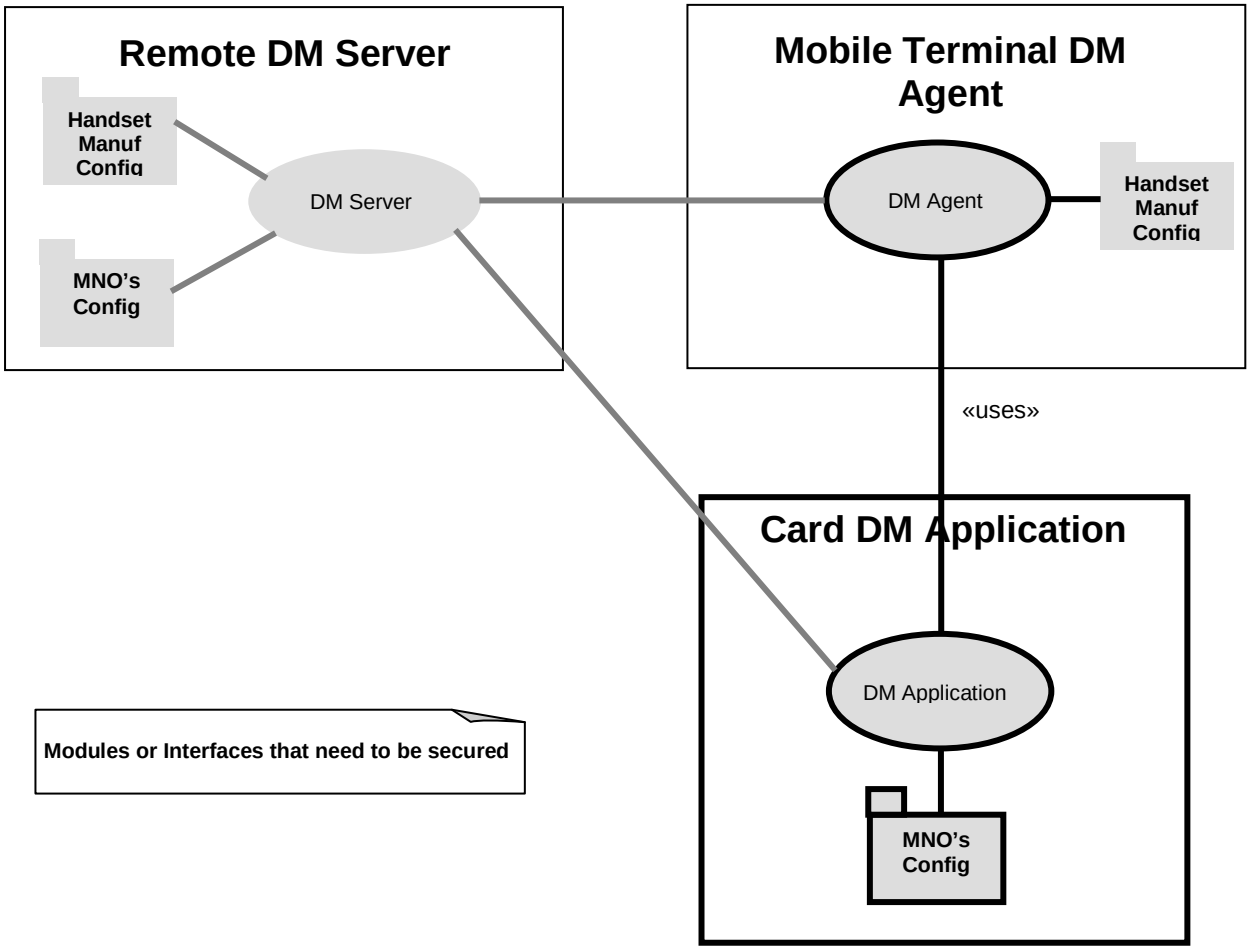


Figure 3: Device Management (DM)

4.5.2.3 Use case - DRM and distributed applications

Digital Rights Management (DRM) is meant to secure media content owned by a service provider; the end-user has a limited set of rights to use the content. Usually, media content is supposed to be rendered on any type of compatible terminal (e.g. CD audio on any CD player) so that the user can transport his content wherever he wants. Adding security should not change this user experience.

In the event the user is a Mobile Network Operator (MNO) subscriber, Open Mobile Alliance (OMA) DRM specifies a model where the rights are bound to a device, not to a user. This implies that when the user needs to change the player (i.e. the handset), the rights have to be downloaded onto the new device and the certificates are to be recalculated with the new terminal ID. This scheme works well as long as a network connection is available and/or the terminal belongs to the same user domain.

A different scheme is proposed, in order to link the rights to a user rather than to the handset: the Rights Object (RO) might be stored in the user's UICC together with part of the DRM user agent. This implies that when the user needs to change the player (i.e. the handset), the rights do not have to be downloaded onto the new terminal. This solution has the following advantages:

1) The user can play content in any MT containing a genuine media player (OMA compatible) and accepting the UICC.

2) The user would not require a network connection. This is useful for situations where the user does not have network coverage (e.g. underground station; plane).

3) The MNO stores its RO in a tamper-resistant device, which is under its control (administration via OTA platform).

This scenario is only possible thanks to the secure channel between a trusted execution environment in the handset and the UICC based DRM User Agent (UA) providing the Content Encryption Key (CEK).

Given that the RO is stored in the UICC, the access to the right can be done directly if the rendering device is the mobile handset (CAD) or, indirectly when the rendering device is a remote terminal (e.g. a Set-Top-Box asking for rights stored in the UICC).

UICC based DRM_UA: the DRM user agent stored in the UICC is there to manage the RO associated to a media content, by managing the parameters and the decryption key (CEK) and by deciding if a content is authorized to be rendered or not.

The session starts by a mutual authentication between the trusted execution environment in the CAD or remote terminal (where the media player is executed) and the UICC based DRM_UA, ending in the opening of a secure channel. Some parameters have to be securely sent to the UICC (trusted time, media content id, etc) so that the DRM_UA can handle the right accordingly (usage counter decrease, etc.) and then securely provide the decrypted CEK to the Trusted Media Player (TMP).

Then the TMP can play the content.

The session is finished when the content has been rendered and the secure channel is closed.

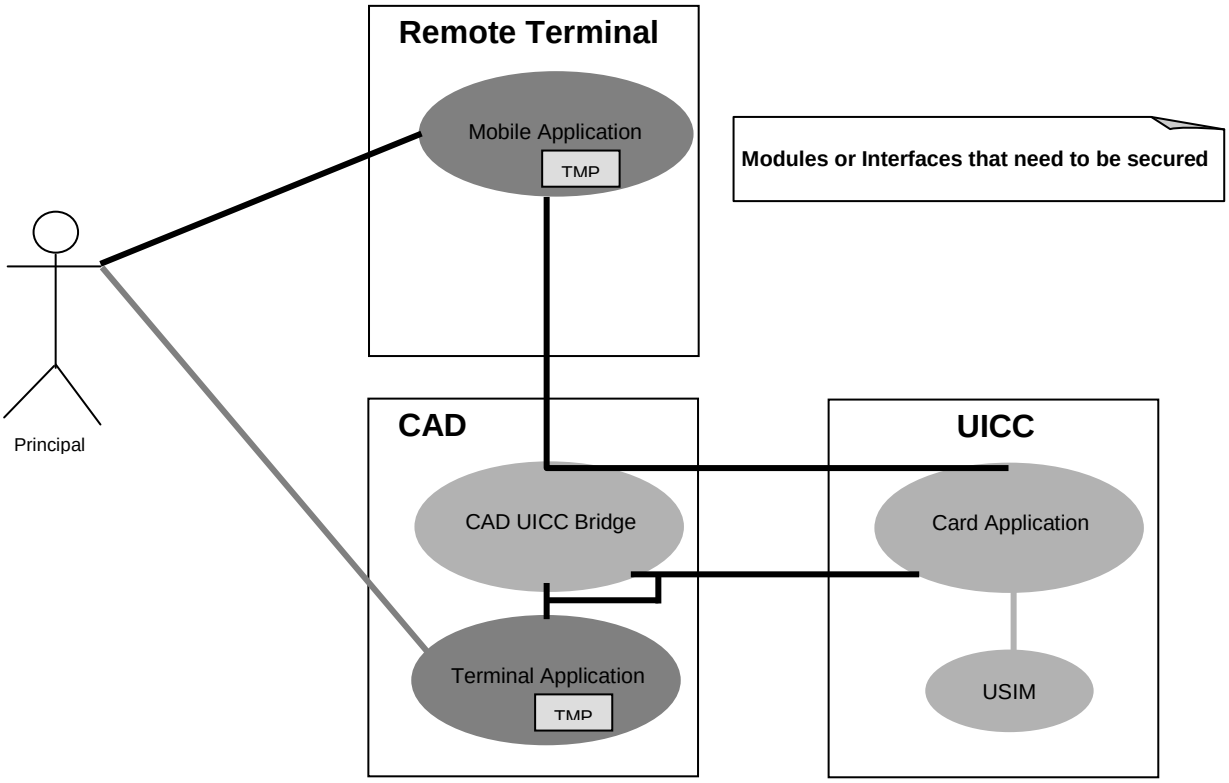


Figure 4: Distributed application

4.5.3 Requirements

This clause describes secure channel's requirements that fit the use cases above.

4.5.3.1 End point requirements

Identifier	Requirement
REQ-7-05-01-01	Applications on the UICC shall be able to establish a secure channel with applications on a terminal (CAD and/or remote terminal). A secure channel in this context is defined in the requirements that follow (see use cases in clauses 4.5.2.1 to 4.5.2.3).
REQ-7-05-01-02	There shall be two different types of end points: • the UICC interface handler and the terminal interface handler (interface end points); • the UICC application and terminal application (application end points).
REQ-7-05-01-03	Through the end points, it shall be possible to establish a Secure Channel per application (see use cases in clauses 4.5.2.1 to 4.5.2.3).
REQ-7-05-01-04	Through the interface end points, several applications on the same terminal shall be able to share the same secure channel with an application on the UICC (see use cases in clauses 4.5.2.1 to 4.5.2.3).
REQ-7-05-01-05	Once a secure channel has been setup between two end points, all communications between those end points shall go via the secure channel.

4.5.3.2 Integrity requirements

Identifier	Requirement
REQ-7-05-02-01	The secure channel shall allow the integrity of the data to be verified (see use cases in clauses 4.5.2.1 to 4.5.2.3).

4.5.3.3 Confidentiality requirements

Identifier	Requirement
REQ-7-05-03-01	Data sent through the secure channel shall be confidentiality-protected depending on the conditions set by the policy (see use cases in clauses 4.5.2.1 to 4.5.2.3).

4.5.3.4 Authentication requirements

Identifier	Requirement
REQ-7-05-04-01	End points of a secure channel shall be able to authenticate each other (see use cases in clauses 4.5.2.1 to 4.5.2.3).
REQ-7-05-04-02	By means of a common trusted third entity, it shall be possible for the UICC end point and terminal end point to agree the keys to be used.
REQ-7-05-04-03	Once keys have been setup, these may be reused, depending on their expiration, to setup a secure channel without reference to a third entity.

4.5.3.5 Audit/Compliance requirements

Identifier	Requirement
REQ-7-05-05-01	The terminal end point shall be a trusted device (see clause 4.5.2).
REQ-7-05-05-02	Evidence shall be provided on the trust ability level of the device. I.e. assessment of the trust ability level shall be possible, for example according to a security certification scheme (see clause 4.5.2).

4.5.3.6 Policy requirements

Identifier	Requirement
REQ-7-05-06-01	An anti-replay mechanism shall be present and active depending on the policy.
REQ-7-05-06-02	It shall be possible to control (e.g. through policy files) what functionality/privileges/access is given to a Terminal end point that has authenticated itself to the UICC end point.
REQ-7-05-06-03	It shall be possible for the terminal owner to control (e.g. through policy files) what functionality/privileges/access is given to a UICC end point that has authenticated itself to the terminal end point.

4.5.3.7 Transport Protocol requirements

Identifier	Requirement
REQ-7-05-07-01	The Secure Channel Protocol should be transport protocol neutral (see use cases in clauses 4.5.2.1 to 4.5.2.3).

4.5.4 Interaction with existing features (informative)

4.5.4.1 Logical Channels

As logical channels exist over the same physical interface, when a secure channel is setup between the UICC interface handler and the terminal interface handler, all communication on any logical channel will go through this secure channel.

4.6 Authenticate command longer than 255 bytes

4.6.1 Abstract (informative)

TS 102 221 [1] specifies only a short length for commands and, therefore large amount of data must be split in several commands, each one no longer than 255 bytes. In this case the protocol becomes inefficient. The situation becomes critical when an authenticate command must be performed.

4.6.2 Background (informative)

4.6.2.1 Use case - EAP packet exchange

A typical situation will be the handling of EAP methods when the EAP packets exceed 255 bytes (e.g. EAP TLS where the packet may be up to 65 536 bytes). This issue cannot be managed today without the definition of a dedicated mechanism or the definition of the extended length command.

Furthermore, the length of the AUTHENTICATE command data is continuously increasing as security needs change.

4.6.3 Requirements

4.6.3.1 General requirements

Identifier	Requirement
REQ-7-06-01-01	A mechanism shall allow the UICC and the Terminal to use an authenticate command even if the data message is longer than 255 bytes.
NOTE: The mechanism introduced should be ISO/IEC 7816-4 [6] compliant.	

4.6.3.2 Backward compatibility requirements

Identifier	Requirement
REQ-7-06-02-01	The authenticate command specified in release 6 and before shall be fully supported by the UICC supporting the new mechanism.
REQ-7-06-02-02	The support of the new mechanism by the UICC shall be indicated to the Terminal.

4.6.4 Interaction with existing features (informative)

(none).

4.7 CAT mechanisms to indicate the bearer connection status

4.7.1 Abstract (informative)

This requirement introduces a new standardized, reliable mechanism in TS 102 223 [2] to provide the UICC with information about the availability of a bearer connection. By means of this new mechanism the UICC knows when it is feasible to start a network related proactive command like Send SM or Setup Call. Current specifications allow the UICC to use several bearers for communication with servers in the network, e.g. SMS and GPRS. The new mechanism shall provide means to indicate and query the status of bearers.

4.7.2 Background (informative)

4.7.2.1 Use case - Availability of network bearers

There are several applications in the field that want to send SM(s) to a server once a mobile station is switched on. One example is an application which checks if the terminal has changed and sends a SMS to a server for Device Management purposes. This type of application needs to be reliably informed at the earliest point in time during the startup of the mobile station when the SM can be sent successfully, i.e. when the network is available. Currently the typical indicator for startup is a Terminal Profile. At the point of time, when the Terminal Profile is sent, some mobiles are neither able to handle proactive commands nor is it guaranteed that access to the network is already available.

4.7.2.2 Use case - Network connection temporarily lost

There are situations where the availability and quality of network connections changes often, e.g. when driving through tunnels or urban areas in a car or in a train. Mobile services which rely on network connections (e.g. in a smartphone or in a PDA equipped with a GSM or UMTS data module) may want to know if a particular network and/or bearer is available or which networks and/or bearers are available before establishing connections and transferring data.

4.7.2.3 Use case - Availability of local bearers

The current standards allow to use local bearers like Infrared, Bluetooth and WLAN to communicate with office equipment in the vicinity. Availability of connections to such equipment may change often when the position of the terminal is changed due to the short range of the connection technology. Mobile applications (e.g. in a smartphone or in a PDA equipped with a GSM or UMTS data module) may want to use these bearers to connect to the office equipment. Having accurate and up-to-date information about the availability of these bearers will simplify the development of applications and will improve the user experience.

4.7.3 Requirements

4.7.3.1 Requirement 1 - Network bearer connection status

Identifier	Requirement
REQ-7-07-01-01	For all supported bearers it shall be possible to set up a list of bearers to monitor connection status.
REQ-7-07-01-02	For all supported bearers it shall be possible to query the status of bearers.

4.7.3.2 Requirement 2 - Local bearer connection status

Identifier	Requirement
REQ-7-07-02-01	For all supported local bearers, indicated in TERMINAL PROFILE, it shall be possible to set up an event to monitor connection status.
REQ-7-07-02-02	For all supported local bearers, indicated in TERMINAL PROFILE, it shall be possible to query the connection status.

4.7.4 Interaction with existing features (informative)

(none).

4.8 New UICC-Terminal interface

4.8.1 Abstract (informative)

Recently UICC memory size has had a very fast growth, from Kbytes up to Megabytes cards that are almost ready for the market today. Certainly this trend will continue in the near future allowing operators to set up a completely new services portfolio.

Next generation services will surely be based on multimedia contents management and the chance to store them inside the card, such as MMS storage on a Rel-6 USIM, will be a key feature. Moreover services related to large data transfer to and from the card, streaming through the card, personalization and control of external devices will need not only large storage capabilities on UICC, but also a fast data access to avoid time latency in service usage granting a better level of user experience and higher connectivity to remote service inside or outside the terminal.

In order to provide these services, some key protocols between UICC and terminal have to be provided.

Although UICC memory and multimedia capabilities have been going to evolve, current UICC-Terminal interfaces did not follow the same evolutionary trend.

Taking into account the above mentioned services evolution, current UICC-Terminal interfaces and protocol stacks shall be revised and New UICC-Terminal interfaces shall be defined and standardized to manage large-sized cards, multimedia Smart Card contents in a faster way and easy connectivity to Internet infrastructure. This new interface shall also be backward compatible with the existing interfaces.

Though the size of storage memory is out of scope of the present document it is felt necessary to warn that memory technologies used in UICCs supporting the new interface might be power hungry and therefore a power negotiation mechanism should be considered necessary.

4.8.2 Background (informative)

Hereafter some use-cases requiring a high-speed dedicated channel between UICC and terminal have been shortly described.

4.8.2.1 Use case - multimedia file management

As the UICC will be able to store and encrypt/decrypt multimedia files (such as MMS, pictures, MP3 files, video clips) customer's usability and Quality User Experience cannot be compromised by a too long wait for the data download/upload. For example it could be of interest to associate an image, a sound and eventually a short video to the information relative to each contact in order to display all the images and video when accessing the phonebook.

4.8.2.2 Use case - MMI on UICC

Large-sized Smart Cards offer the possibility to store card issuer's MMI in the UICC. During initialization process, the terminal can detect the type of UICC (which operator, which service providers, which features) and upload the whole MMI that the card issuer has defined for its purposes and its services. This operation should be performed only if a New UICC is detected by the terminal. This operation shall be performed as fast as customer's experience would not be affected. A mechanism to identify the detection of a new UICC should be standardized.

4.8.2.3 Use case - real-time multimedia data encryption/decryption

UICC can be used to directly encrypt/decrypt data stream (such as protected voice communications or streamed video and music). For example the user should be able to receive multimedia files (e.g. Audio or Video) encrypted using rights stored inside the UICC. Both the content and its decryption key should be stored in the UICC and also the decryption process could be executed inside the card. The decrypted content could be offered via a streaming protocol in order to increase the level of security. In addition the user could also store personal contents in the UICC and send them after having protected them through encryption features of the UICC.

An additional use case requiring very similar capabilities of the interface is the signature of multimedia documents, as it is not necessary for the UICC to store the document in order to compute the signature as the document is streamed through.

4.8.2.4 Use case - storage of terminal applications on the UICC

UICC could be used to store and distribute applications that could be uploaded by the terminal during the initialization phase or later. The uploading from the UICC to the terminal (or vice versa) of the applications should happen dynamically according to user rights purchased from the operator. This enables efficient management of operator-related applications on the terminal and easy deployment of innovative services on the field.

4.8.2.5 Use case - direct and indirect UICC connection to a PC

As it is now possible for some devices it should be possible either to insert a UICC directly into a PC laptop or to connect the handset to PC laptop in order to download/retrieve some personal data (MMS, pictures, movies, applications, etc.) to/from the card in a very quick time but also to easily execute cryptographic operations for accessing a secure environment (e.g. PKI for e-commerce). The user should consider the UICC as his trusted storage device, ensuring acceptable performances for the targeted use.

In case of an indirect connection to a PC, the UICC to PC connection should be targeted to be independent from the host operating system. Security of the UICC to PC link shall be guaranteed.

4.8.2.6 Use case - web server on Smart Card

UICC can be considered like a web server to which an Internet connection can be established with a usual Internet browser. Such a solution removes the needs of deployment of middleware to interface the functionality of the UICC as standard browsers and protocols would be used to access UICC contents and applications.

Contents will be both stored and dynamically generated on the Smart Card and then transferred to the terminal: the aim is to reuse standard graphic features of handsets to allow mobile operators to offer attractive and secure services. A quick communication interface between the terminal and the UICC will enhance the web server performances; TCP/IP based communication allows internal pages (in the UICC) to be served locally and remotely using standard protocols and methods. The operation of insert, delete or modify shall be performed in a very fast way so that customer's experience would not be affected.

Through a web server it will be possible to offer a new range of services such as the possibility to access UICC files (e.g. the phonebook, the MP3 and videos list) via a web interface in order to consult or modify them.

4.8.2.7 Use case - antivirus on UICC

The usage of the UICC as a storage device or the downloading on it of new applications and services lead to the need of antivirus running on the UICC itself, like it happens in a PC environment. The UICC could be able to perform auto-scan, to update virus signature or managing user rights and the New UICC-Terminal interface should not affect this functionality with a too slow definition files download.

4.8.2.8 Use case - big phonebook management from the UICC

Big memory cards will offer the opportunity to provide big phonebooks portability with some additional parameters (such as voice activated dialling). The usage of this extra UICC capability should be transparent for the end user thanks to a fast exchange of data between the UICC and the terminal. The phonebook data needs to be accessible through each of the interfaces of the UICC allowing for administration through either interface.

4.8.2.9 Use case - reduce personalization time

As memory of the card increases, more data needs to be written during personalization e.g. prior to card issuance. The new interface can be used to personalize the card, e.g. to load Smart Card applications to the UICC in a reasonable time.

4.8.2.10 Use case - generic TCP/IP connectivity

Many services can be built using the user's UICC as a trust-enabling device. From that standpoint, it is highly beneficial that the New UICC-Terminal interface provides support of TCP/IP as this enables the use and integration of the UICC in IP networks as an endpoint. The Smart Card Web Server and the Liberty Alliance use-cases are good candidates for the use of such generic TCP/IP connectivity.

4.8.3 Requirements

4.8.3.1 General requirements

Identifier	Requirement
REQ-7-08-01-01	The New UICC-Terminal (NUT) interface parameters shall be capable of providing 8 Mbps (net interface speed without protocol overheads and re-transmissions).
REQ-7-08-01-02	The New UICC-Terminal interface shall offer technical solutions to evolve to higher speed rates with backward compatibility, and be open for future needs (SCP release 8 and onward).
REQ-7-08-01-03	A mechanism shall be provided to detect the presence of the NUT interface. If no NUT interface is detected, the terminal shall select the ISO/IEC interface.
REQ-7-08-01-04	If both the terminal and the card support the NUT interface, the terminal shall select the NUT interface.
REQ-7-08-01-05	The NUT interface shall provide a proactive mechanism to initiate communication with the terminal and/or the network.
REQ-7-08-01-06	At least one of the plug-in and mini UICC form factors from a dimensional point of view (width, height and thickness) shall be able to accommodate the NUT interface.
REQ-7-08-01-07	The NUT interface shall be able to support the use of higher level protocols (such as HTTP and TCP/IP) in order to provide connectivity to existing infrastructures.
REQ-7-08-01-08	After the NUT interface has been activated by the terminal, a higher power consumption can be negotiated.
REQ-7-08-01-09	An UICC supporting the NUT interface shall support the ISO/IEC interface.
REQ-7-08-01-10	The NUT interface shall be able to support streaming data.
REQ-7-08-01-11	It shall be possible to run authentication commands through the NUT interface without affecting the existing timing constraints.
REQ-7-08-01-12	The NUT interface being present on a UICC shall not conflict with the possibility of having an additional contact-less connectivity solution.
REQ-7-08-01-13	The NUT interface being active shall not prevent activity taking place on additional connectivity solutions (if present) nor affect responsiveness on this connectivity solution (e.g. swipe mode contact-less transactions).
REQ-7-08-01-14	The New UICC-Terminal interface shall not degrade security on the UICC.
REQ-7-08-01-15	When the NUT interface is used to run only pre-Rel-7-commands, the default UICC power shall not exceed what is specified in TS 102 221 [1] specifications.
REQ-7-08-01-16	The introduction of the NUT interface shall not modify the existing form factors (as defined in TS 102 221 [1]) causing a separate reader to be required.
REQ-7-08-01-17	The power consumption of the UICC including the interface when all activities are stopped shall not exceed the currently specified value for clock stop mode.
REQ-7-08-01-18	To introduce a NUT interface, no new contacts in addition to the 8 contacts specified in ISO/IEC 7816-4 [6] series are to be added to the UICC.
REQ-7-08-01-19	The use of some of the currently assigned contacts in the SCP specification and non-assigned contacts (C4, C6, C8) should be negotiable to allow the limited resources available to be used in the most flexible way.
REQ-7-08-01-20	There shall be a mechanism to negotiate power consumption of the NUT interface based on the used speed.
REQ-7-08-01-21	The NUT interface parameters shall offer a predictable scalability mechanism.
REQ-7-08-01-22	A UICC supporting the NUT interface shall be able to be activated under class C operating conditions/supply voltage until adequate operating conditions are negotiated between the UICC and the terminal if needed.

4.8.3.2 Backward compatibility requirements

Identifier	Requirement
REQ-7-08-02-01	The New UICC-Terminal interface shall be backward compatible with the existing interfaces. It shall be possible to use a new interface-based UICC with a pre-Release 7 terminal according to pre-Release 7 specifications.
REQ-7-08-02-02	For backward compatibility reasons and in order to preserve the handset's battery time, the UICC shall keep its power consumption within the range defined in TS 102 221 [1] Release 6 unless the New UICC-Terminal interface is activated.
REQ-7-08-02-03	The assignment and use of currently non-specified contacts in SCP specifications (C4, C6, C8) is not to cause unpredicted operation of the UICC when inserted into an existing terminal, the fact that some contacts are left unconnected or connected to a specific level shall not cause operational problems.

4.8.4 Interaction with existing features (informative)

(none).

4.9 UICC based application acting as a server

4.9.1 Abstract (informative)

A connectivity solution to the hosting device is required to enable a client in the terminal to retrieve data from a web server running in the UICC.

4.9.2 Background (informative)

A Smart Card Web Server can be used to transfer static pages to be displayed to the user.

A Smart Card Web Server can be used to dynamically generate some pages to be displayed to the user.

Content stored in the Smart Card Web Server can be updated by a client in the terminal.

4.9.3 Requirements

Identifier	Requirement
REQ-7-09-01-01	A connectivity solution shall be provided to enable a client in the terminal request data from a web server in the UICC.
REQ-7-09-01-02	This connectivity solution shall provide a general transport mechanism for HTTP and HTTPS.
REQ-7-09-01-03	This connectivity solution shall not reduce the security of other UICC applications (e.g. SIM, USIM, ISIM…).
REQ-7-09-01-04	This connectivity solution shall not prevent Card application toolkit sessions from operating simultaneously with the Smart Card Web Server sessions.
REQ-7-09-01-05	This connectivity solution shall be able to handle multiple simultaneous sessions to the UICC.
REQ-7-09-01-06	This connectivity solution shall allow to transport HTTP requests and responses which are longer than 255 bytes.

4.9.4 Interaction with existing features (informative)

(none).

4.10 API for applications registered to a Smart Card Web Server

4.10.1 Abstract (informative)

A Web Server on the Smart Card (SCWS) receives requests from a client and provides HTML content as a response. This content can either be static or dynamic.

Dynamic content can be created by the web server itself or by special applications in the Smart Card (servlet-like applications). In order to extend the functionality of the SCWS it is necessary to load these special applications (which create dynamic content on behalf of the web server) to the Smart Card after issuance.

4.10.2 Background (informative)

A service provider wants to use the Smart Card of a user as an authentication device. He develops an application, which computes the response to a challenge using a key in the application and asks his operator to install it in the Smart Card of the user.

The user browses a page of the service provider and receives a page with a link to the Smart Card Web Server. When the user clicks on this link, a request is issued to the SCWS, where the URL contains the name of the application and the challenge as a parameter.

The Smart Card invokes the application of the service provider, which computes the response to the challenge and returns a page to the web server, which is returned to the browser and displayed. This returned page contains a link to the service provider, which includes the response to the challenge in the URL. When the user clicks on this link, the response is sent within the URL to the service provider.

4.10.2.1 Registration of an application to the SCWS

When the operator installs the application of the service provider it registers under a given name to the Smart Card Web Server.

4.10.2.2 Data exchange between SCWS and application

When the application is invoked by the SCWS the challenge is passed to the application.

After the dynamic content is created by the application, it is passed back to the SCWS. The SCWS returns this response page as the result of the request.

4.10.2.3 Issuing Proactive Commands

Applications registered to the SCWS need to be able to generate and send proactive commands to the terminal. The application that has sent the proactive command needs to evaluate the corresponding terminal response. Sending of the proactive command and evaluating the terminal response will be possible while the application creates the dynamic content.

4.10.3 Requirements

Identifier	Requirement
REQ-7-10-01-01	There shall be a mechanism to register and de-register an application to a Smart Card Web Server.
REQ-7-10-01-02	It shall be possible to perform registration/de-registration of an application separately from its installation/un-installation (not necessarily excluding the possibility for a combined register/install or de-register/uninstall mechanism).
REQ-7-10-01-03	There shall be a secure mechanism to allow a Smart Card Web Server to invoke a registered application.
REQ-7-10-01-04	There shall be a secure mechanism to allow a Smart Card Web Server to pass parameters to a registered application.
REQ-7-10-01-05	There shall be a secure mechanism to allow a registered application to return data to a Smart Card Web Server.
REQ-7-10-01-06	These mechanisms shall be available in form of an API for Java Card Applets.
REQ-8-10-01-07	There shall be a mechanism, if possible an existing one, that allows applications registered to the SCWS to generate and send proactive commands and to receive the corresponding terminal response while creating dynamic content.

4.10.4 Interaction with existing features (informative)

(none).

4.11 Specific UICC environmental conditions

4.11.1 Abstract (informative)

The mobile telecommunication industry is extending its business beyond the existing communication services offered by normal handsets. For example, automotive service, machine-to-machine communication and RFID are possible services and estimated to become a large market in the near future. For such new business areas, various types of mobile terminals are required to be developed for each environment and those terminals are likely to be used at times in a harsh environment compared to the normal handset. For a harsh environment such as in cars, machines and outdoors, electrical equipment is generally required to have much reliability to conform to its usage environment, which is also applicable to the UICC.

The use cases and requirements for specific UICC environmental conditions listed below are optional features of the UICC.

4.11.2 Background (informative)

This clause lists use cases relevant to specific UICC environmental conditions.

4.11.2.1 Use case - Automotive service

Mobile communication integration with automotive service will be expected to become a large market in the future. A mobile terminal embedded in the car navigation system can offer various services such as interactive information (traffic and shop, etc) services, remote car diagnosis services, automatic emergency reporting and remote navigation using video call.

4.11.2.2 Use case - Remote monitoring camera

Remote images can be monitored in real-time by setting a camera with a mobile terminal at a certain location. Examples of these types of demands are monitoring of children in the nursery school, pets left at home, monitoring of mountains, rivers and coastal regions for disasters such as typhoon, flood, volcano and earthquake. In some cases, these terminals are placed outdoor and exposed to the open air conditions.

4.11.2.3 Use case - Remote stock monitoring for vending machines

The mobile terminal is embedded in a vending machine, which can communicate with the monitoring server. When stocks become low, the machine automatically conveys this to the server, so that the staff can replenish the product in the vending machine. The terminal has to be able to work in outdoor conditions.

4.11.2.4 Use case - Online electronic advertising board

Advertising contents can be automatically managed and updated by a delivery server using a mobile communication network. The electronic board can be set anywhere, e.g. on top of the buildings, on the street or in the station.

4.11.3 Considerations (informative)

The UICC is the key component in the mobile terminal. If it does not operate due to temperature or ambient harsh environment, mobile communication service itself cannot be offered. Therefore the reliability on environmental conditions should be taken into consideration.

4.11.4 Requirements

4.11.4.1 Requirement 1: Temperature range

Identifier	Requirement
REQ-7-11-01-01	The temperature range for specific environmental conditions shall be classified according to its range.
REQ-7-11-01-02	The temperature class A shall be defined as the temperature range for card operation specified in TS 102 221 [1].
REQ-7-11-01-03	The temperature class B for full UICC operational use and storage shall be between -40 °C and +85 °C.
REQ-7-11-01-04	The temperature class C for full UICC operational use and storage shall be between -40 °C and +105 C.
REQ-7-11-01-05	The temperature class D for full UICC operational use and storage shall be between -40 °C and +125 °C.
REQ-7-11-01-06	Temperature classes other than class A shall be optional, allowing manufacturers to choose the class according to the application.
REQ-7-11-01-07	It shall be possible for the UICC to indicate its temperature class to the terminal. If there is no indication of temperature class, that shall be interpreted as temperature class A.

4.11.4.2 Requirement 2: Humidity

Identifier	Requirement
REQ-7-11-02-01	Optionally it should be possible to qualify the operation of the UICC in an environment with high humidity.
REQ-7-11-02-02	The qualification shall be for operational usage and storage of the UICC at 90 % to 95 % Relative humidity throughout the temperature range up to +85 °C.

4.11.5 Interaction with existing features (informative)

(none).

4.12 Introduction of high density memory technology in UICC

4.12.1 Abstract (informative)

The addition of a high-speed interface to the card will enable proper user-experience regarding any service dealing with a large amount of data stored on the card. Therefore, such large memory cards will appear and they will need to be manufactured using available memory technology.

There is a strong expectation from the handset manufacturers to use voltage class "C" in the future.

Today, these memory technologies do not allow for compliance with existing UICC power constraints (both current and class "C" voltage).

In order to be able to use such cards, additional electrical conditions may be needed.

4.12.2 Background (informative)

4.12.2.1 Use case - Enhanced UICC features

The card provides the subscriber with a larger amount of memory, allowing for enhanced UICC features:

- Addition of new fields in the phonebook.
- Larger amount of phonebook entries.
- Storage of large files such as multimedia files, messages.
- Other personal information.

4.12.3 Requirements

Identifier	Requirement
REQ-7-12-01-01	A mechanism shall be defined or adapted if necessary so that the UICC is able to indicate its electrical needs (current and voltage) to the terminal.
REQ-7-12-01-02	A mechanism shall be defined or adapted if necessary so that the UICC is informed of the capability of the terminal to support its electrical needs (current and voltage).
REQ-7-12-01-03	The mechanisms defined in REQ-7-12-01-01 and REQ-7-12-01-02 shall be included in the initialization of the UICC.
REQ-7-12-01-04	For backward compatibility, the UICC shall be compliant with pre-Rel-7 features, and in particular with the electrical characteristics, if the mechanism defined in REQ-7-12-01-02 is not supported by the terminal or if the terminal cannot provide the voltage and/or current values required by the UICC. In this last case the UICC functionality based on high density memory shall not be available if it exceeds pre-Rel-7 (TS 102 221 [1] R6) voltage and current requirement.
REQ-7-12-01-05	In case a new voltage class is introduced the system impact shall be analysed and the impact kept to a minimum.

4.12.4 Interaction with existing features (informative)

(none).

4.13 Power supply indication mechanism

4.13.1 Abstract (informative)

Currently TS 102 221 [1] specifies that a UICC application may specify its own maximum power consumption values up to a maximum value as specified in the table 6.3. In the same clause it also states that a terminal shall be able to supply at least the values of power consumption indicated in the table 6.4. It means that there are terminals in the field which supply the power consumption to the UICC in a range from the minimum (see TS 102 221 [1], table 6.4) up to the maximum (see TS 102 221 [1], table 6.3). If the terminal is not able to supply the power consumption requested by the UICC then the application may not work properly. In order to avoid this problem it is mandatory that the UICC application requires a value of power consumption which the mobile is able to supply. The problem is that there is no mechanism which informs the UICC application about the maximum value of power consumption the terminal is able to supply.

In the case where the terminal is not able to supply the value of power consumption requested by the UICC application it is useful if the UICC application can reduce its power consumption requirements by deactivating power consuming parts of its application or by lowering its performance to stay operational. Therefore the UICC application need to be informed before its selection about the available power supply of the terminal to react accordingly.

4.13.2 Background (informative)

4.13.2.1 Use case - generic situation

A typical situation will be that on the UICC several applications (e.g. USIM, ISIM, WIM, toolkit applications, etc.) are installed. If one or more applications need a value of power consumption higher than the minimum one specified in TS 102 221 [1], table 6.4 (but still within the range defined in TS 102 221 [1], table 6.3), then the application has to indicate in the response of a SELECT or STATUS command the power consumption value needed. If the terminal is not capable of delivering this power supply then a mechanism to inform the UICC is missing and therefore the application cannot work properly and no mobile communication is possible.

4.13.2.2 Use case - USIM application with toolkit applications

The most important application on an UICC within a 3G mobile phone is the USIM application necessary for mobile communication. Even if under normal circumstances this application requires a value of power consumption inside the range of TS 102 221 [1], table 6.4, typically additional toolkit applications associated with the USIM application are installed to provide additional services to the mobile phone user. Such toolkit applications could require an increase of the overall power consumption to a value higher than the guaranteed minimum supplied by the terminal (e.g. application using USSM for asymmetric cryptography). As the toolkit applications are not directly selected by the terminal, the USIM application would, in this case, have to request a higher power consumption during its selection.

In a situation where the USIM would require a power consumption higher than the maximum value indicated by the terminal, the USIM application shall remain operational and has to provide basic network functionality.

If the application running on the UICC can identify the maximum possible power supply delivered by the terminal then it may adjust its maximum power consumption inside of terminals with limited power supply by one of the following actions to guarantee its operation:

a) It deactivates application parts consuming more power (e.g. toolkit application).

b) It reduces its performance of power consuming parts (e.g. by dividing the CPU clock).

4.13.3 Requirements

4.13.3.1 General Requirements

Identifier	Requirement
REQ-7-13-01-01	A mechanism shall be introduced that informs the UICC about the maximum power consumption supported by the terminal.
REQ-7-13-01-02	The power consumption indication mechanism shall be mandatory for a Release 7 terminal (or higher) able to provide more than the minimum power consumption.
REQ-7-13-01-03	The power consumption indication mechanism shall be optional for Release 7 terminal (or higher) providing only the minimum power consumption (see note).
REQ-7-13-01-04	In the case where the power consumption indication mechanism is supported by the terminal, the UICC shall be informed about the maximum power consumption before the first application selection command.
NOTE: It is recommended that Release 7 terminal with minimum power supply offer the power consumption indication mechanism.	

4.13.3.2 Backward compatibility requirements

Identifier	Requirement
REQ-7-13-02-01	The power consumption indication shall not generate backward compatibility issues with pre-Release 7 UICCs and terminals.
REQ-7-13-02-02	A UICC capable of receiving this indication shall stay with the minimum power consumption if no indication is given by the terminal.

4.13.4 Interaction with existing features (informative)

(none).

4.14 Internet Connectivity up to UICC applications

4.14.1 Abstract (informative)

There is a need to define a new way to connect UICC applications to other Internet applications.

If this can be achieved in multiple technical ways, it is clear that there is a need to rationalize the way the UICC will exchange data with the external world and ease the integration into terminals by avoiding the need to translate in a terminal middleware from one protocol to another.

4.14.2 Use Cases (informative)

The operators want to use the UICC with the following services, e.g.:

- Access (for modification or consultation) to the end user personal data stored in the UICC.
- Access from a personal computer using a local link.
- Access from a remote entity to an authentication application running on the card.

4.14.2.1 Use Case - Card OTA management

Remote management of the UICC by operators is complex and has limitations due to today's connection method (SMS or CAT-TP). UICCs with large amounts of memory are hitting the market. As an example, a basic phone personalization file containing menus, icons, screen savers, background pictures may be 1 Megabyte. A full update of this kind of file could be performed with a fast and efficient protocol between the remote management server and the UICC. Widely used internet protocols for large file transfer or synchronization may be used up to the card, using existing web infrastructures and software.

The card may act as server, in which case the remote management system will take the initiative to establish the connection to the card. Establishing such a remote connection to the card is the most efficient way to enable instantaneous updates.

If the card acts as a client, the remote management system will have to trigger an update from the card or have to rely on a periodic inquiry from the card, which leads to inefficient bandwidth usage and unpredictable update delays. SMS or WAP push may be used to trigger synchronization.

4.14.2.2 Use Case - User local access from the terminal to a card server

UICC contains a web server to which an internet connection can be established with a browser in the terminal. This allows to address content management on the UICC without installing specific drivers on the host terminals.

Content is both stored and dynamically generated on the smart card and then transferred to the terminal: The aim is to re-use standard graphic features of handsets to allow mobile operators to offer attractive and secure services. The operations of insert, delete or modify shall be performed on user data such as phonebook entries so that customer's experience is not affected.

It will be possible to offer a new range of services, such as the possibility to access UICC files (e.g. the phonebook, the MP3 and videos list) through a web server via a web interface in order to consult or modify them. Some examples are listed below:

a) Dick wants to purchase a gift for his father's birthday while he is in public transportation coming back from work. While browsing the internet on his mobile terminal in search for a gift, he finds a book that is well suited to his father's interests. Dick just has to click on the "payment" icon. His UICC transparently initiates a strong mutual authentication with the payment server securing the transaction. The UICC requests Dick to enter his PIN code to perform the authentication and secure the purchase process with the back-end server. While Dick is browsing, a small UICC icon appears on his browser (like the padlock on PC browsers) to let him know that the transaction is secured by the UICC. Nothing has been stored on the handset during the transaction. Dick can lend his handset to a friend without any worry.

b) Jack has been offered a new handset. As this handset was not part of an operator's bundle, no setup was performed in the factory for Jack's network operator. Jack inserts his UICC and displays the help topics from his UICC with the handset's browser. A nice animated tutorial tells Jack about the way to input the parameters that have not already been synchronized from the UICC to the handset. Jack can now take full advantage of his handset on his operator's network.

c) Mike's new UICC comes out with some advertising web pages (e.g. the operator agreed selling advertising space to other companies) preloaded, that may also be accessed offline. Since it is appealing Mike is induced to browse the web pages available on the UICC. If he finds/needs some service/information related to the advertising service he asks for it and the connection is established at this stage.

4.14.2.3 Use Case - Remote access to an identity server in the card

The UICC is the primary carrier for digital user identity. A connected UICC will be used as an identity provider not only on the wireless network but on the wide internet allowing operators to offer new applications and business models. There is a need for the UICC to enable to authenticate the remote entity.

Relevant use cases are addressed separately.

4.14.2.4 Use Case - User access from a locally connected device to a card service

Access to the UICC from a PC connected to the wireless terminal will expand the use cases of the UICC up to the PC and the IT world. Support for standard protocols such as HTTP or SyncML will allow an easy management of SIM content from a user's PC without deployment of phone vendor specific applications. The UICC must be able to authenticate the attached PC and to be able to filter requests based on connection identifiers.

Relevant use cases are addressed separately.

4.14.3 Requirements

Identifier	Requirement
REQ-7-14-01-01	It shall be possible to establish an IP based connection to the UICC from a local entity.
REQ-7-14-01-02	It shall be possible to establish an IP based connection to the UICC from a remote entity.
REQ-7-14-01-03	It shall be possible to use an end-to end Internet security protocol with the UICC (e.g. IPSEC or TLS).
REQ-7-14-01-04	UICC applications shall be able to act in client mode and in server mode.
REQ-7-14-01-05	Establishing a connection with the UICC should preferably not require any changes to existing internet infrastructures and applications running on remote entities that want to establish connections with the UICC.
REQ-7-14-01-06	There shall be a mechanism to guarantee the access of the UICC from an application using a text label that is common for all UICC access.
REQ-7-14-01-07	There shall be a mechanism for the UICC to provide name(s) to the terminal that can then be used instead of the default name or the IP address and port number to access the UICC.

4.14.4 Interaction with existing features (informative)

(none).

4.15 Contactless UICC services

4.15.1 Abstract (informative)

Contactless card technology is gaining importance on the market. Recent developments also allow mobile terminals and the UICC contained in the terminals to take part in contactless communication.

This clause lists the use cases and resulting requirements for a contactless enabled UICC, where the latter acts as a trusted device in the contactless environment.

4.15.2 Background (informative)

This clause lists use cases relevant for Contactless UICC Services.

Implementing contactless services in the mobile and the UICC enhances the user experience, for example by adding MMI capabilities, and it enables remote administration of these services (application download, personalization, administration, etc.).

4.15.2.1 Use case - Access

4.15.2.1.1 System aspects of use case

Contactless Access Systems exist today. These are based on a wide range of contactless technologies; a significant number of which are based on ISO/IEC 14443 [8] types A and B. There are few standards in this area, these systems vary by supplier and may be customized for specific customers.

The Access Systems can be categorized into 2 groups:

a) Access device tolerated unavailability - These systems have secure entry and/or exit using a contactless device or via an alternative process (e.g. The user is tolerant to the contactless device being unavailable).

b) Access device mandated availability - These systems have secure entry and/or exit using a contactless device only (e.g. The user is not tolerant to the contactless device being unavailable).

4.15.2.1.2 UICC role in use case

The UICC based device has the ability to operate as three types of device within this use case:

Card Emulation Cases:

a) Access Request Device - Access device tolerated unavailability. This device is carried by the user and is used by the user to request access to the areas that the user is allowed in. In this instance the device operates in Contactless card emulation mode and it is expected that any required user interface will be part of the reader device. There are many different access schemes that the UICC needs to be compatible with to deliver this use case, so it is important that the Access Request Device is highly customizable. To aid this customization, information about the air interface used and the terminal capabilities need to be available to the UICC application environment. The user expects the application to inform them of any issues when it is a new terminal configuration.

   In this use case, it is acceptable to the user to use alternative access methods if the Terminal - UICC combination are not in "normal operation" mode for the terminal. This use case does not mandate operation under special operating conditions (such as no terminal power).

b) Access Request Device - Access device mandated availability. This device is carried by the user and is used by the user to request access to the areas that the user is allowed in. In this instance the device operates in Contactless card emulation mode and it is expected that any required user interface will be part of the reader device. There are many different access schemes that the UICC needs to be compatible with to deliver this use case, so it is important that the Access Request Device is highly customizable. To aid this customization, information about the air interface used and the terminal capabilities need to be available to the UICC application environment. The user expects the application to inform them of any issues when it is a new terminal configuration.

In this use case, the user requires the Terminal - UICC combination to have a comparable functionality and user experience whatever the power state of the host device (i.e. mobile handset containing the UICC).

Reader Emulation Case:

c) Access Manager Device - This device is used by a manager of the access system to manage the system and the devices within it. There are typically fewer instances of the Access Manager Device in a system compared to the Access Request Device. In this instance the Access Manager Device operates in Contactless card reader mode or "peer to peer" mode and it is expected that any required user interface will be part of the Terminal - ICC device. There are many different access schemes that the UICC need to be compatible with to deliver this use case and many different types of "system manager", so it is important that the Access Manager Device is highly customizable. To aid this customization, information about the air interface used and the terminal capabilities need to be available to the UICC application environment.

As the terminal user interface is being used, the user only expects the Access Manager Device to operate under "normal operating conditions" (e.g. The user does not expect operation when the terminal power is unavailable).

The user expects that the Access Manager Device can communicate with all Access Grant Devices without the need for additional power connection.

UICC applications written to implement the Access Manager Device may require interaction with other parts of the access infrastructure. Therefore this use case expects that the Contactless aspect of the Terminal - UICC device and the Terminal - UICC devices air interfaces shall be available simultaneously.

For all access use cases, the UICC contains the application and data required for continuous or temporary access to a secured area like company buildings. The data and applications may be loaded, pre-configured or revoked using an off-line device or provisioned remotely through the telecom network.

4.15.2.2 Use case - tickets

The Ticket Use case can be split into two types of Contactless ticketing with different properties:

- Transport ticketing:
  Many public transport schemes now use contactless readers and cards for access to and use of, the transport system. These are based on a wide range of standards (ISO/IEC 14443-A, ISO/IEC 14443-B [8], Philips MiFare, Felica, etc.).

- Event ticketing:
  There is growing number of venues using contactless ticketing for events (e.g. Sporting venues and exhibition venues). There are no clear standards in this area.

Both ticketing schemes have two potentially conflicting priorities to be accounted for in the UICC, which are detailed below as two corresponding scenarios:

- Speed of throughput - getting people through a gate as fast as possible, typically using low cost tickets.

- Fraud protection, usually associated with medium or high priced tickets - Preventing loss of money due all types of fraud, particularly identity fraud. (e.g. someone "borrowing" somebody else's season ticket). In this scenario tickets can be either:

  - stored in the ticketing infrastructure and the identity of the user in the UICC, it should be kept in mind that there is typically a high volume of tickets in a ticketing system;

  - stored in the UICC.

4.15.2.2.1 System aspects of throughput ticketing scenario

Tickets can be purchased and stored securely on the UICC. A single purchase can result in multiple tickets. Tickets are typically of low value. The systems associated with this type of scenario do not typically allow tickets to be exchanged between cards.

UICC based Throughput Ticketing offers both the transport systems and the mass event systems (e.g. large attendance sports events) cheaper way of implementing a contactless ticketing system (fewer issued contactless cards and potentially less retailer commissions) and the user a more convenient way to carry a contactless ticket and more flexible purchase experience.

4.15.2.2.2 System aspects of high priced ticketing scenario

Tickets can be purchased and stored securely on the UICC. In view of the (medium to) high value of the tickets, The UICC based implementation must provide adequate protection mechanisms (e.g. to make it useless to steal someone's phone to enter an event). The UICC based ticket may need the system to authenticate itself before each ticket can be viewed, used or deleted. The ability to view and legitimately and securely transfer tickets is potentially an added benefit for tickets stored in a UICC (as compared with a "classical" Contactless card).

For this type of scenario, UICC based ticketing offers to the issuers of these tickets a cheaper way of implementing a contactless ticketing systems (a one off contactless smartcard may be too expensive for a single event, or for every individual high priced transport ticket/pass type) thus enabling the advantages of smartcard over paper tickets. For the user, UICC based ticketing should offer a more convenient and secure way to carry ticket and more flexible purchase experience.

4.15.2.2.3 UICC role in use case

The UICC based device has the ability to operate as three types of device within this use case:

Card Emulation Cases:

a) Throughput ticket device. This device is carried by the user and is used by the user to access an event or use transport. The user interface and mechanisms for this ticket are focused on speed of access. In this instance the device operates in Contactless card emulation mode and it is expected that any required user interface will be part of the reader device. There are many different existing ticketing schemes that the UICC needs to be compatible with to deliver this use case, so it is important that the Access Request Device is highly customizable. To aid this customization, information about the air interface used and the terminal capabilities need to be available to the UICC application environment. The user expects the application to inform them of any issues when it is a new terminal configuration.

   The UICC is used to store and manage tickets securely in this use case, so there is a need for secure storage of potentially a large number of tickets and authentication mechanisms to validate reader requests.

   In this use case, it is not acceptable to the user to use alternative access methods if the Terminal - UICC combination are not in "normal operation" mode for the terminal. This use case requires operation under special operating conditions (such as no terminal power).

b) High value ticket device. This device is carried by the user and is used by the user to access an event or use transport. The user interface and mechanisms for this ticket are focused on protecting the ticket and the system from illegal activity. In this instance the device operates in Contactless card emulation mode and it is expected that the terminal user interface may be used to validate the identity of the user using the ticket or to manage/view the ticket. There are many different access schemes that the UICC needs to be compatible with to deliver this use case, so it is important that the Access Request Device is highly customizable. To aid this customization, information about the air interface used and the terminal capabilities need to be available to the UICC application environment. The user expects the application to inform them of any issues when it is a new terminal configuration.

   The UICC is used to store and manage tickets securely in this use case, so there is a need for secure storage of potentially a large number of tickets and authentication mechanisms to validate reader requests and the user. Additionally, mechanisms to allow the transfer of tickets from one user to another are needed along with a prevention mechanism to stop this transfer if the system forbids it.

   In this use case, the user requires the Terminal - UICC combination to have a comparable functionality and user experience whatever the power state of the host device (i.e. mobile handset containing the UICC) unless additional security is being offered.

Reader Emulation Case:

c) Ticket Management Device - This device is used by an inspector verify a ticket and the identity of its holder (where applicable). There are typically much fewer instances of the Ticket Management Device in a system compared to the Throughput Ticket Device and High Value Ticket Device. In this instance the Ticket Management Device operates in Contactless card reader mode or "peer to peer" mode. It is expected that any required user interface will be part of the Terminal - UICC device and that the UICC will have the identity, authentication and validation mechanisms required. There are many different access schemes that the UICC need to be compatible with to deliver this use case and many different types of "system manager", so it is important that the Access Manager Device is highly customizable. To aid this customization, information about the air interface used and the terminal capabilities need to be available to the UICC application environment.

   As the terminal user interface is being used, the user only expects the Ticket Management Device to operate under "normal operating conditions" (e.g. The user does not expect operation when the terminal power is unavailable).

   The user expects that the Ticket Management Device can communicate with all scheme Ticket Devices (both UICC based and non-UICC based) without the need for additional power connection.

   UICC applications written to implement the Ticket Management Device may require interaction with other parts of the access infrastructure. Therefore this use case expects that the Contactless aspect of the Terminal-UICC device and the Terminal - UICC devices air interfaces shall be available simultaneously.

For all ticket use cases, the UICC contains the application and ticket/identity information. The data and applications may be loaded, pre-configured or revoked using an off-line device or provisioned remotely through the telecom network.

4.15.2.3 Use case - digital rights

4.15.2.3.1 System aspects of contactless digital rights

DRM systems can allow the content to be stored separately from the rights. The UICC is an ideal secure environment to allow a user to carry their digital rights. To use these rights, users need to be able to communicate with content players equipped with Contactless DRM. Additionally, users need the ability to legally transfer (gift) these rights to other users (where allowed). An easy way to facilitate the transfer/exchange of rights is via a contactless interface.

4.15.2.3.2 UICC role in use case

A mobile handset with UICC based Contactless provision has the ability to operate as two types of device within this use case:

Card emulation case:

a) DRM Store device. This device is carried by the user and is placed within range of a supporting content player to allow content to be played that the user has paid for. In this instance the device operates in Contactless card emulation mode and but it is expected that any required user interface will be part of the UICC - Terminal device.

   The UICC is used to store and manage DRM rights securely in this use case, so there is a need for secure storage of potentially a large number of rights and authentication mechanisms to validate reader requests.

   In this use case, it is acceptable to the user to use alternative access methods if the Terminal - UICC combination are not in "normal operation" mode for the terminal. This use case does not require operation under special operating conditions (such as no terminal power).

   Existing secure OTA mechanisms together with UICC based applications may be used to process the payment and download digital rights onto the UICC.

b) DRM Transfer device - This device is used by a user to transfer DRM rights to another user (where allowed). In this instance the DRM Transfer Device operates in Contactless card reader mode or "peer to peer" mode. It is expected that any required user interface will be part of the Terminal - UICC device and that the UICC will have the identity, authentication and validation mechanisms required.

As the terminal user interface is being used, the user only expects the Ticket Management Device to operate under "normal operating conditions" (e.g. The user does not expect operation when the terminal power is unavailable).

UICC applications written to implement the Ticket Management Device may require interaction with other parts of the access infrastructure. Therefore this use case expects that the Contactless aspect of the Terminal - UICC device and the Terminal - UICC devices air interfaces shall be available simultaneously.

4.15.2.4 Use case - payment application

Card emulation mode:

- The UICC contains the application and data required for contactless payment application.

  The terminal containing the UICC in this scenario has two possibilities:

  - It can act like a contactless payment application to pay at a contactless-enabled Point Of Sale (POS).
  - It can act as a proxy for a payment account in which a third party performs a debit transaction, passing the payment to the merchant.

Existing secure OTA mechanisms together with UICC based applications may be used to load, modify or update payment application information on the UICC, depending on permissions.

Reader emulation mode:

- The UICC may not contain the application and data required for a contactless payment application use, but rather the merchant credentials. The actual data and application for a payment application is contained in another contactless card external to the terminal. In this case, the mobile terminal may operate in reader mode and be used as a remote PIN pad when the contactless payment card is close to the terminal.

4.15.2.5 Use case - loyalty application

Card emulation mode:

- The UICC contains the application and data required for loyalty application.
- The terminal containing the UICC can act like a contactless loyalty application at a contactless-enabled Point Of Sale (POS).
- Existing secure OTA mechanisms together with UICC based applications may be used to load, modify or update loyalty application information on the UICC, depending on permissions.
- The service would have the same basic loyalty functionality whatever the UICC powering mode.

Reader emulation mode:

- The UICC may not contain the application and data required for a loyalty application use, but rather the merchant credentials. The actual data and application for a loyalty application is contained in another contactless card external to the terminal. In this case, the mobile terminal may operate in reader mode and be used as a remote PIN pad when the contactless loyalty card is close to the terminal.

4.15.2.6 Use case - health care application

Card emulation mode:

- The UICC contains the application and data required for a health care application.
- The terminal containing this UICC is used to store medical and health insurance data. These essential data would be available whatever the powering mode of the UICC. The use of the contactless interface may occur in places where strict security or safety rules apply (e.g. regulations requiring a terminal to be switched off in a hospital).

Reader emulation mode:

- Moreover, the handset device, through the contactless interface, may transfer specific credentials and data from medical equipment to the UICC, allowing patients to keep this data up to date and transfer data between doctors or hospitals. This would only work if the UICC is battery powered. Of course, this data may be read, written or updated according to security rules.

4.15.3 Requirements

4.15.3.1 Physical interface requirements

Identifier	Requirements
REQ-7-15-01-01	The CLFI being present on the UICC shall not conflict with the possibility of having a high-speed solution.
REQ-7-15-01-02	The CLFI being present on the UICC shall not conflict with the possibility of having a TS 102 221 [1] solution.
REQ-7-15-01-03	The solution shall be compatible with the existing form factors as defined in TS 102 221 [1].
REQ-7-15-01-04	The CLFI shall be compatible with the battery powered mode.
REQ-7-15-01-05	The CLFI shall be compatible with the not battery powered mode in card emulation mode.
REQ-7-15-01-06	There shall be a means for the UICC to detect the nature of its power source.
REQ-7-15-01-07	The CLFI shall allow for optimized power management.

4.15.3.2 Multi-protocol concurrent operation requirements

Identifier	Requirements
REQ-7-15-02-01	The UICC shall be capable of managing concurrently communication using both legacy protocol defined in TS 102 221 [1] and the CLFIP.
REQ-7-15-02-02	The UICC shall be capable of managing concurrently communication using both HSP and the CLFIP.

4.15.3.3 Contactless communication modes requirements

Identifier	Requirements
REQ-7-15-03-01	The CLFI and the CLFIP shall allow the system consisting of the UICC and the terminal to behave as a contactless card.
REQ-7-15-03-02	The CLFI and the CLFIP shall allow the system consisting of the UICC and the terminal to behave as a contactless reader.
REQ-7-15-03-03	The CLFI and the CLFIP shall allow the system consisting of the UICC and the terminal to support "peer to peer" mode as specified in ISO/IEC 18092 [9].

4.15.3.4 Compatibility with existing contactless systems requirements

Identifier	Requirements
REQ-7-15-04-01	The CLFIP shall allow the transport of data of communication protocols compatible with existing infrastructures based on the following standards: • ISO/IEC 14443 [8] -A and -B. • ISO/IEC 18092 [9].
REQ-7-15-04-02	The CLFIP shall be flexible enough to transport data for other RF protocols than those listed in REQ-7-Y-04-01. • Example: ISO/IEC 15693 [10].
REQ-7-15-04-03	The system consisting of the UICC and the CLF shall consider multi-cards and multi-applications environments.

4.15.3.5 Parameters to be transported by the CLFIP requirements

Identifier	Requirements
REQ-7-15-05-01	The CLFIP shall be capable of providing the UICC with RF field state: • Example: presence of field.
REQ-7-15-05-02	The CLFIP shall provide a parameter negotiation mechanism: • Example: speed, protocol type, automatic interface detection, power modes supported, RF mode capabilities.

4.15.3.6 Application integration requirements

Identifier	Requirements
REQ-7-15-06-01	It shall be possible to activate and deactivate the accessibility and visibility of the contactless based applications on the UICC.

4.15.3.7 Terminal and user interaction requirements

Identifier	Requirements
REQ-7-15-07-01	In battery powered mode, it shall be possible for the CLFIP to signal that the UICC request to start a proactive session at any time, or that a user interaction is required.
REQ-7-15-07-02	The CLFIP shall allow the transport of a request for CLF allocation.

4.15.3.8 Interoperability requirements

Identifier	Requirements
REQ-7-15-08-01	Interoperability between the UICC and the CLF shall be guaranteed.
REQ-7-15-08-02	If the card reader mode is using the CLFIP, the same protocol stack shall be used for both card emulation and reader modes if possible (with the exception of mode-specific commands).

4.15.4 Interaction with existing features (informative)

The dedicated hardware link for the CLFI has direct impact on the current discussion for a high speed interface between the terminal and the UICC, because there is only a limited number of currently unused contacts on the UICC.

4.16 Administration of the Smart Card Web Server

4.16.1 Abstract (informative)

The content provided by the Smart Card Web Server may be statically stored in the UICC memory, or it may be dynamically generated by an application in the UICC.

To allow an application in the UICC to dynamically generate content for the Smart Card Web Server, there is a need to transmit requests to specific URIs received by the Smart Card Web Server to the appropriate applications. This implies the possibility for an application to register itself to the Smart Card Web Server and to request to map/unmap itself to a specific URIs.

4.16.2 Background (informative)

A card issuer may want to provide an application that generates dynamic content whenever the user makes a request to an associated URI in the Smart Card Web Server. When the application is installed on the UICC of the user, possibly over the air after issuance of the UICC to the user, an administrative APDU sent to the UICC indicates that this application shall be mapped to a specific URI in the Smart Card Web Server.

4.16.3 Requirements

Identifier	Requirement
REQ-8-16-01-01	There shall be a mechanism to map an application in the UICC to a URI within the SCWS.
REQ-8-16-01-02	There shall be a mechanism to remove the mapping of an application in the UICC with a URI within the SCWS.
REQ-8-16-01-03	The above mechanisms shall be available in the form of an administrative APDU available over the air.

4.16.4 Interaction with existing features (informative)

(none).

4.17 Confidential Application Services

4.17.1 Abstract (informative)

With the advent of protocols that allow the UICC to interact with terminal applications, there is a growing need for UICC issuers to "rent space" on a UICC to third parties. Usually all the applications that run on the UICC are fully managed by the card issuer.

This clause specifies requirements and use cases for a set of services that will allow third party application developers to develop services, based on the UICC API, in a way that the card issuer cannot inspect the code. Services and requirements are also specified that allow the card issuer to manage the rights of third party application developers and possibly restrict third party application functionalities.

The third party applications developed according to the following requirements are referred as "confidential applications".

4.17.2 Background (informative)

4.17.2.1 Use case 1: Mobile TV services

A Mobile TV service is a service which allows to broadcast TV and MultiMedia content through the air interface by using an appropriate set of frequencies and appropriate TV systems and standards such as DVB-T, DMB, MBMS, …, and to receive all the broadcast channels by using a mobile terminal which acts as a TV decoder and screen display. When the terminal is a mobile handset able to provide access to GSM and/or 3G networks at the same time, the customer can be attached to a mobile network and receive Mobile TV broadcast channels at the same time, being both a mobile customer and a Mobile TV customer.

Some of the Mobile TV broadcast channels can be protected and encrypted so that only the customer with a valid Mobile TV subscription has the grants to receive, decrypt, decode and display the contents. All the other customers can receive the broadcast but not to decrypt it (so the broadcast content cannot be properly displayed by the terminal).

Most of these systems (referred as Conditional Access Systems, or CAS) are using the UICC as one of the protection elements, storing a CAS application dealing with:

- the security algorithm that is responsible to generate the temporary keys to be used by the terminal application to decrypt the broadcast stream;
- the storage and management of customer's licences;
- other security issues.

In order to provide protection and encryption, specific companies are owners of the Mobile TV broadcast encryption system (CAS) and are responsible of it in case the system will be cracked. In fact when a broadcast system is cracked, in the worst case all the users can have access to the protected stream without being authorized. If the system is patched, it could be necessary to modify the system itself (algorithms, keys,…) and then provide brand new UICCs to all (or a part of) the customers to keep on accessing the protected broadcast streams.

The CAS provider has the following "needs":

- the possibility to develop a highly secured performance UICC application;
- the possibility to provide additional proprietary algorithms to manage all the CAS issues;
- the possibility to generate keys during the life time of the UICC;
- the possibility to load the application and its data onto the card in a confidential mode, so that neither the card issuer nor the card owner is able to decode and reverse engineer the CAS applet itself;
- the possibility to securely upgrade the CAS applet or its data via Over-The-Air mechanisms;
- the possibility to securely patch the CAS applet via Over-The-Air mechanisms.

Specifically the CAS company needs to protect its system, based on its own proprietary algorithm (for instance), based on its own proprietary mode of generating the temporary keys to be used to decrypt the broadcast stream of data, based on its proprietary mode to assign a specific customer address (a set of parameters to uniquely identify the customer and his grants, that is which channels and which programs he is able to decrypt, and the time and duration of these credentials).

At the same time the card owner does not want to load an application on his own card without knowing which is the exact behaviour of that.

The card owner has the need:

- to enable or disable the CAS applet via Over-The-Air mechanisms;
- to restrict (or control) the functionalities of the CAS applet, for instance:
  - controlling file access (for instance disabling and enabling for specific files);
  - controlling the usage of some specific CAT/USAT commands (e.g. to disable the possibility to issue Send SMS, Set Up Calls, …);
  - controlling the priority of commands, for instance to run the authentication command within the network timing constraints.
- to build firewalls between the CAS applet and all the other applications on the UICC (so that the CAS applet shall not be able to interfere with the UICC owner profile and applications) and vice-versa;
- to control part of the requested CAS applet resources (RAM memory allocation requests, temporary object allocation requests, number of requested logical channels, permanent object allocation memory request, …);
- to interrupt the CAS applet execution in case the UICC performances should be degraded too much;
- to have CAS applets that are interoperable between different card platforms.

4.17.2.2 Use case 2: Banking Services

A Banking application is an application typically used to set up an end-to-end protected and encrypted link between the UICC and the Bank server, by-passing all the Mobile Operator network elements.

The banking application can potentially be connected to the Bank server in several ways:

- via the Mobile Operator network;
- locally connected to a POS (via Bluetooth, NFC, ZigBee, …);
- via a Wi-Fi network inside a Bank area (potentially protected environment);
- via a Wi-Fi network outside a Bank area (potentially unprotected environment);

In order to provide an end-to-end protected link to the Bank, the third party application should manage some information such as:

- storage of keys into the UICC (these keys shall not be accessible by the card issuer);
- storage of specific customer-related data (customer identification,…);
- possibly define proprietary algorithms and protocols to manage the end-to-end connection;
- possibly interact with external peripherals (Bluetooth,…);
- possibly interact with a locally connected POS.

The banking confidential application developer has mainly the following "needs":

- a secure operating environment that firewalls the banking applications from all other applications. This may need to be certified;
- the possibility to develop a highly secured performance UICC application;
- the possibility to provide additional proprietary algorithms to manage the end-to-end connection;
- the possibility to store/generate keys during the life time of the UICC;
- the possibility to load the application and its data onto the card in a confidential mode, so that neither the card issuer nor the card owner is able to decode and reverse engineer the banking confidential application itself;
- the possibility to upgrade the application or its data via Over-The-Air mechanisms (or via a local connection of the handset with a PC);
- the possibility to patch the application via Over-The-Air mechanisms;
- the possibility to request the user to digit PIN codes and in general to interact with the terminal user interface (display messages, request input, send and receive data through SMS and GPRS and UMTS bearer,…);
- the possibility to interact with external peripherals such as Bluetooth (for instance to be connected to a POS) or USB connection to PC;
- the possibility to interact with a contactless interface to send/receive data through it.

At the same time the card owner needs to be confident that the banking application will not harm or interfere with the card owners applications and functions.

The card owner has the need:

- to enable or disable the banking confidential application via Over-The-Air mechanisms;
- to restrict (or control) the functionalities of the banking confidential application, for instance:
  - controlling file access (for instance disabling and enabling for specific files);

  - controlling the usage of some specific CAT/USAT commands (e.g. to disable the possibility to issue Send SMS, Set Up Calls, …);
  - controlling the priority of commands, for instance to run the authentication command within the network timing constraints.

- to build firewalls between the banking confidential application and all the other applications on the UICC (so that the banking application shall not be able to interfere with the UICC owner profile and applications);
- to manage part of the requested banking confidential application resources (RAM memory allocation requests, temporary object allocation requests, number of requested logical channels, permanent object allocation memory request, …);
- to be able to recover operation of the card if a third party application has not released resources;
- to have banking confidential applications that are interoperable between different card platforms.

4.17.2.3 Use case 3: Contactless Applications

The use of Confidential applications is particularly relevant for all of the contactless use cases described in clause 4.15.

For specific contactless application deployment, for example when the application is dedicated to payment, there is a possibility to introduce a new actor in the ecosystem: the Trusted Service Manager (TSM) [i.1]. This entity is primarily responsible for securely distributing, provisioning and life-cycle management of the payment application to the mobile network operators' subscriber base, on behalf of the service providers. The TSM will have business relationships with both the mobile network operators and the service providers, and is in charge to implement requirements of both entities. In this respect, the TSM administrate one (or several) third party area in the UICC and performs the overall management of the third party areas, according to the security policy definition.

In this case, the card owner needs:

- to delegate some management rights to the TSM;
- to have the capability to restrict rights to the TSM.

In this case, the TSM needs:

- to create third party area for service providers;
- to delegate some management rights to the service providers.

4.17.2.4 Use case 4: Mobile Virtual Network Operator services

The UICC is a key tool used by UICC issuers and MVNO's to customize the end customer user experience. Through use of the current file based features of the UICC, a completely re-branded experience can be achieved. Whilst file customisation is catered for within ETSI specifications, there is currently no means for a UICC issuer to grant the MVNO rights to use other card resources such as SIM Toolkit and the UICC API without compromising the UICC issuer security.

This use case enables the UICC issuer to grant MVNOs access to UICC resources and functionality in a controlled and secure way through the reservation of a third party secure area (third party area) on the UICC where the MVNO's applications can be securely allocated.

The UICC issuer will be able to administrate the third party area by the use of the following features:

- reserve a third party secure area on the UICC for the use of each MVNO (as it is possible for an MVNO to host another MVNO on the same UICC);
- fully or partially remove and recover resources of the third party area that were previously assigned;
- suspend a third party area (this may be required if a contract temporarily lapses or if a security issue arises);
- fully or partially allocate or extend resources assigned to a third party area;

- interrogate the UICC to detect which UICC resources have been allocated to each third party area;
- generate/Load administration keys for distribution that allow the MVNO to load and create other third party areas;
- to restrict (or control) the functionalities of the third party areas and of the applications loaded on that area, for instance:
  - controlling file access (disabling and enabling specific files);
  - controlling the usage of some specific CAT/USAT commands (e.g. to disable the possibility to issue Send SMS, Set Up Calls, …).
- to build firewalls between the third party area application and all the UICC issuer applications (so that the third party area application shall not be able to interfere with the UICC owner profile and applications) and vice-versa;
- to control part of the requested third party area application resources.

The UICC issuer will not be able to:

- Use secure resources allocated to the third party area (e.g. Keys, counters).
- Interrogate, install or retrieve any applications loaded by the MVNO.
- Deactivate or remove any individual MVNO application.

The MVNO will be able to:

- create secure objects in the third party area that the UICC card issuer has no access to;
- load and fully manage applications loaded by the MVNO;
- interrogate the UICC to establish the available resources in the third party area;
- use all card resources that the UICC issuer has enabled for that third party area;
- create and administrate further areas within the allocated third party area allowing the MVNO to host MVNOs itself.

The MVNO will not be able to:

- use UICC features not explicitly enabled by the card issuer;
- use any resources outside of the third party area.

4.17.3 Requirements (normative)

This clause defines the requirements for confidential applications.

4.17.3.1 Confidential application environment

Identifier	Requirements
REQ-8-17-01-01	A UICC conforming to this feature shall be able to set up at least one third party area.
REQ-8-17-01-02	Third party areas shall be firewalled from each other.
REQ-8-17-01-03	Third party access to files and procedures outside of the third party area shall be limited by the mechanisms described for this feature.
REQ-8-17-01-04	The card issuer shall not be able to install, delete, or disable individual applications or specific data in a third party area.
REQ-8-17-01-05	Third party applications shall not be able to prevent other applications (card issuer applications, other third party applications,..) from successful operation.
REQ-8-17-01-06	A third party application shall not delay the UICCs response to an AUTHENTICATE command.
REQ-8-17-01-07	A third party area shall have its own file system and sufficient APIs to allow data manipulation, file manipulation (limited to its own files) and security functions (limited to its own keys).
REQ-8-17-01-08	There shall be a mechanism to allow the card issuer to set the maximum response window of a third party area.

4.17.3.2 Administration by Card issuer

4.17.3.2.1 Third party area environment administration

Identifier	Requirements
REQ-8-17-02-01	A card issuer shall be able to manage third party areas by the following means: • At personalisation • Securely over the card interface • Securely over the air
REQ-8-17-02-02	A card issuer shall be able to create 1 or more new third party areas.
REQ-8-17-02-03	A card issuer shall be able to disable a third party area.
REQ-8-17-02-04	When a third party area is disabled by the card issuer, all third party features, including administration, shall be disabled.
REQ-8-17-02-05	A card issuer shall be able to re-enable a third party area.
REQ-8-17-02-06	A card issuer shall be able to remove a third party area.
REQ-8-17-02-07	The process of removing a third party area shall ensure that all data, including applications, files and keys, shall be erased irrevocably.
REQ-8-17-02-08	A card issuer shall be able to set the policy for the third party area.
REQ-8-17-02-09	The card issuer shall be able to recover memory released due to a policy change affecting the required memory.
REQ-8-17-02-10	A card issuer shall be able to retrieve the policy for each third party area.
REQ-8-17-02-11	There shall be an optional mechanism for the card issuer to be able to retrieve a list of installed applications that are registered in a central repository.
REQ-8-17-02-12	The list of installed applications shall contain AID, URI or URL information.

4.17.3.2.2 Third party area creation

Identifier	Requirements
REQ-8-17-03-01	The card issuer shall set the size of the memory available to the third party area.
REQ-8-17-03-02	Third party areas shall be firewalled from their creation.
REQ-8-17-03-03	There shall be a mechanism available to allowing the UICC to generate administration key values for a third party area.
REQ-8-17-03-04	There shall be at least one mechanism defined that allows the third party area administration keys to be delivered from the UICC to the third party, securely and without these being discoverable by the card issuer.
REQ-8-17-03-05	There shall be at least one mechanism defined that allows the third party area administration keys to be downloaded from an off-card entity to the third party area, securely and without these being discoverable by the card issuer.

4.17.3.2.3 Third party area policy definition

Identifier	Requirements
REQ-8-17-04-01	The third party policy shall include its maximum memory allowance for the third party volatile and non-volatile memory.
REQ-8-17-04-02	The third party policy shall include its allowed access to UICC security domains.
REQ-8-17-04-03	The third party policy shall include its allowed access to key sets and associated key sets.
REQ-8-17-04-04	The third party policy shall include its allowed access to the files in the UICC.
REQ-8-17-04-05	The third party policy shall include its allowed access and restriction to APIs at a package level.
REQ-8-17-04-06	The third party policy shall include its allowed access and restriction to specific proactive CAT commands.
REQ-8-17-04-07	The third party policy shall include its allowed access to application identifiers (such as TARs, url, uri, …).
REQ-8-17-04-08	The third party policy shall include its allowed access and restriction to the number of concurrently selected third party applications in the third party area.
REQ-8-17-04-09	The third party policy shall include its allowed access to other UICC interfaces such as contactless or the ethernet emulation and mass storage classes of the USB interface.

4.17.3.3 Administration by Third party

Identifier	Requirements
REQ-8-17-05-01	All third party areas shall have a management capability that allows third parties to administrate their third party area (e.g. loading and deletion of application, managing application lifecycle, managing security data such as keys or security domain).
REQ-8-17-05-02	The third party shall be able to fully administrate the file system and applications within their third party area.
REQ-8-17-05-03	The third party shall be able to retrieve the policy settings for this third party area.
REQ-8-17-05-04	The third party shall be able to disable and delete its own third party area.
REQ-8-17-05-05	The third party shall be able to re-enable its own third party area if it disabled it.
REQ-8-17-05-06	When a third party area is disabled by the third party, the third party administration shall not be disabled, only operation of application and access to data contained in third party area will be disabled.
REQ-8-17-05-07	There shall be a mechanism that allows the card issuer to transport encrypted third party administration messages on behalf of the third party.
REQ-8-17-05-08	There shall be a mechanism for the third party to register or de-register an application from a central repository (e.g. EF_DIR,…).

4.17.3.4 Service Operator specific requirements

The Service Operator is a generic word covering the MVNO role as defined in MVNO usecases (when managing third party area for other MVNO) and the Trusted Service Manager role defined for Contactless usecase. The Service Operator shall be considered as a third party compliant with the following set of requirements.

Identifier	Requirements
REQ-8-17-06-01	The implementation of the Service Operator specific requirements is optional but, if implemented, shall be provided as a complete set.
REQ-8-17-06-02	The card issuer shall be able to set the permission for a third party area to have sub-third party areas.
REQ-8-17-06-03	A third party that has permissions to have sub-third party areas shall setup sub-third party areas being sub-divisions of its third party area.
REQ-8-17-06-04	A third party that has permissions to have sub-third party areas shall be able to administer the permissions for the sub-third party areas, which will be a subset of its third party permissions.
REQ-8-17-06-05	The sub-third party shall be able to fully administer the file system and applications within its own sub-third party area, being compliant with its permissions.
REQ-8-17-06-06	Any restriction by the card issuer to third party permissions shall also apply to the sub-third party areas permissions.

4.17.4 Interaction with existing features (informative)

This feature may impact the following UICC features:

- Existing APIs.
- SELECT mechanism specified in TS 102 221 [1].
- Card Application Toolkit TS 102 223 [2].

4.18 UICC for Machine-to-Machine (M2M) applications

4.18.1 Abstract (informative)

Machine-to-Machine (M2M) is a generic expression which describes applications where a machine is communicating via a mobile communication system automatically or on demand with another machine or a background system. M2M is a growth sector and will continue to be so, particularly in mature markets. The ubiquitous coverage of mobile networks is an enabler for this growth.

M2M addresses a number of market segments, including the automotive industry, vending, metering, payment terminals and tracking devices. Therefore there is a need to update the requirements of the UICC to meet these industry market criteria. This clause will focus on a collection of UICC platform requirements addressing those various market segments for all M2M UICC form factors and the requirements for a new form factor for the UICC (MFF) for cases where the current UICC form factors are not appropriate.

Although, there are a large number of possible use cases, these can currently be broadly categorised into 4 major groups; Track and Trace, Monitoring, Transaction and Control.

The communication via the mobile communication system is performed by a M2M communication module which is connected to a UICC. A M2M communication module is an electronic system including all necessary components to establish wireless communications between machines. M2M communication modules are usually integrated directly into target devices, such as Automated Meter Readers (AMRs), vending machines, alarm systems, cars equipments or others.

In many of the intended use cases there are specific requirements related to the size, shape, environmental conditions, vibrations etc.

In all these use cases there might be the need for applications running either in a M2M communication module, a UICC or be split between the two.

4.18.2 Use Cases (informative)

4.18.2.1 Use case - Track and Trace

Track and trace use cases are mainly automotive related. M2M applications within the automotive industry are focused on delivering enhanced security for people (emergency call applications) or assets (theft tracking applications). Fleet management applications focus on increased operational efficiency and increased incremental revenue. These services are broad ranging and include remote diagnostics, navigation systems, pay-as-you-drive (insurance, in-car services), etc.

For use cases in the automotive sector there are common automotive criteria. The Automotive Electronics Council (AEC) was established for the purpose of establishing common part-qualification and quality-system standards directly addressing product reliability. The AEC Component Technical Committee is the standardization body for establishing standards for reliable, high quality electronic components.

The automotive market increasingly requires that semiconductor suppliers provide products compliant to the AEC-Q100 [i.3] standard and ISO 16750 [i.2] (provides guidance regarding environmental conditions commonly encountered by electrical and electronic systems installed in automobiles) as such the M2M UICC may comply with all appropriate requirements, more specifically:

- with AEC-Q100 [i.3] (AEC-Q100 stress test qualification for automotive integrated circuits) requirements and be delivered with PPAP (Production Part Approval Process) documentation.
- with class E as defined in ISO 16750-3 [i.2].

4.18.2.1.1 Use case - Emergency Call

The in-vehicle emergency call system can save lives by automatically or manually sending the accurate location and driver information to an emergency centre. In this use case, an in-vehicle M2M communication module enables the transfer of emergency call data between the vehicle and an emergency service.

In this use case, a vehicle has a built-in M2M communication module which is connected to sensors that can identify an occurring accident. In case of an accident the module automatically sets up a connection to an emergency centre and sends information about the location, an indication about the level of the accident and maybe other additional information that might be available and evaluated as useful. These services may be implemented via applications residing inside the M2M UICC. A key criterion for this use case is that the M2M UICC and its interface to the module are able to survive and operate after a shock caused by an accident. Additionally, the automotive industry has indicated that the size of the M2M UICC and module and the ability of the module to communicate whilst in a normal automotive environment, over the expected vehicle lifetime, are important.

This use case may imply specific requirements for the M2M UICC including:

- temperature and humidity according to the specific requirements of the automotive industry;
- able to operate, whilst attached in a module, withstanding normal automotive vibration;
- designed for a product lifetime of over 10 years with high usage;
- size and form factor to minimise the overall size of the M2M communication module;
- size and form factor to allow automated pick and place of the MFF;
- the ability the make it difficult for the user to remove or misuse the device;
- application interaction between M2M UICC and remote sensors (FFS).

4.18.2.1.2 Use case - Fleet Management

For this use case, a vehicle has a built-in M2M communication module which is typically owned by a company (not the user). The module collects information, for example: location, timings, traffic jams, maintenance data and transport environmental conditions. This information can be sent by the module via a mobile network to a server application where it can be used to track the vehicle and deliveries.

Using the retrieved information, a server application can effectively optimise the delivery plan and route. The adjusted delivery plan is then sent via the mobile network to the vehicle and appropriate information can be displayed to the driver. Additionally, based on the maintenance related information, maintenance can be planned or remote maintenance performed. In addition, environmental sensors can be used to retrieve information on the storage environment and condition of product being transported. These services may be implemented via applications residing inside the M2M UICC.

Key criterion for this use case is the ability of the M2M communication module to communicate whilst in a normal automotive environment, over the expected vehicle lifetime.

This use case may imply specific requirements for the M2M UICC including:

- temperature and humidity according to the specific requirements of the automotive industry;
- able to operate, whilst attached in a module, withstanding normal automotive vibration;

- designed for a product lifetime of over 10 years with high usage;
- size and form factor to minimise the overall size of the M2M communication module;
- size and form factor to allow automated pick and place of the MFF;
- the ability the make it difficult for the user to remove or misuse the device;
- application interaction between M2M UICC and remote sensors (FFS).

4.18.2.1.3 Use case - Theft Tracking

Currently, the theft of automobiles is usually prevented in one of two ways, either by deterring the thief with an alarm system or by preventing the engine from starting with an immobiliser system. These systems however can be evaded, for example by quickly disabling or ignoring the alarm system, or transporting the vehicle without the aid of the engine.

In this use case the introduction of the M2M UICC allows for the possibility of preventing the theft itself or recovering the vehicle, for example by theft tracking. It is envisioned that the M2M UICC in a module will allow secure communication over the network to a third party entity. In the future the UICC may even take part in securing the vehicle.

The M2M UICC in this use case will have to function in an extended temperature and humidity range not usual for a terminal. In addition, the connection between the M2M UICC and the M2M communications module will have to withstand the vibration produced by the engine of the vehicle as well as by the vehicle on the road. To keep the M2M UICC from suffering the same fate as numerous alarm systems, it needs to be protected against theft and misuse, for example through M2M UICC to vehicle and/or communications module pairing.

Another factor in this environment is the often limited space available to conceal or secure the system from theft and misuse, which means that the size of both the M2M communications module and the M2M UICC itself must be kept small. In order to make it available to a large segment of the automobile market, in some cases, the M2M UICC will have to be integrated in mass produced modules as generally required by the automobile manufacturer groups. As vehicles are built to have a lifetime that may easily extend beyond ten years, but also keeping the costs of maintenance to a minimum, lifetime expectation is also a factor for the UICC.

This use case may imply specific requirements for the M2M UICC including:

- protection of the M2M UICC against theft and/or misuse by e.g. M2M UICC to device pairing;
- secure communication over the network to a third party entity;
- size and form factor to minimise the overall size of the M2M communication module;
- size and form factor to allow automated pick and place of the MFF;
- temperature and humidity according to the requirements of the automotive industry;
- able to operate, whilst attached in a module, withstanding normal automotive vibration;
- designed for a product lifetime of over 10 years with;
- application interaction between M2M UICC and remote sensors (FFS).

4.18.2.2 Use case - Monitoring

M2M applications within this category are either used to monitor and control utilities consumption, or monitor, track and trace persons, animals or assets.

4.18.2.2.1 Use case - Metering / Prepaid delivery of utilities (water, gas, electricity)

The utility companies deploy intelligent metering services by installing M2M communication modules on metering devices which can send information automatically or on demand to a server application which can, for example, be used to automatically bill the metered resource. These services may be implemented via applications residing inside the M2M UICC.

In this use case the purpose is either to improve energy performance and efficiency through the delivery of a much more accurate picture of consumption, efficiency and cost, while also delivering the end user actual usage without human intervention. This in turn provides a positive environmental impact. In the opposite direction information inside the metering device may be securely updated over the air.

Metering devices are often placed in harsh environments. This requires that the M2M UICC has to withstand these environmental conditions, e.g. extreme temperatures or humidity. In many metering devices space is very limited, meaning the size of the M2M communication module needs to be minimised, which requires also the size of the M2M UICC to be minimised. Metering devices may be produced in high volumes, which requires that the M2M UICC can be integrated in an industrialised process. As sensitive data might be stored, the module including the M2M UICC needs to be protected against theft and misuse.

This use case may imply specific requirements for the M2M UICC including:

- temperature and humidity according to the specific requirements of the metering industry;
- protection against theft and misuse by e.g. M2M UICC to device pairing;
- the lifetime of a meter is often more than 15 years with frequent usage (read/write cycles);
- size and form factor to minimise the overall size of the M2M communication module (some applications need small meter add-ons to provide communication capability once the devices are in the field);
- size and form factor to allow automated pick and place of the MFF;
- application interaction between M2M UICC and remote sensors.

An extension of the above use case for metering of gas, electricity, water, is based on pre-payment. A household can purchase a specific volume of gas, electricity, water, etc. by pre-payment. The information about the purchased volume is securely transmitted over the air to the metering device and then securely stored inside the M2M UICC. During consumption the actual information about the consumed volume is transmitted to the M2M UICC. When the purchased volume has been consumed the supply can be stopped.

This use case implies the ability to perform secure transactions between the M2M UICC and the controlled metering device. This may also include the possibility to securely perform control operations e.g. stopping the delivery.

4.18.2.2.2 Use case - Person / Animal protection

In this use case persons and / or animals are equipped with portable devices containing a M2M communication module, an M2M UICC and optionally a GPS function, which sends information automatically or on demand to a server application which can monitor the status and positioning of the persons or animals. The purpose is to improve security and / or remotely monitor the status while also being able to track and trace either the person or the animal. These services may be implemented via applications residing inside the M2M UICC.

For persons, the typical applications are lone worker, healthcare, elderly or child monitoring. For animals, the typical application is track and trace.

The portable devices are often placed in harsh environments; this means that they are undergoing strong vibrations or even shocks. The connection between the M2M communication module and the M2M UICC has to withstand these vibrations or shocks. The space is very limited, meaning the size of the M2M communication module needs to be minimised, which requires also the size of the MFF to be minimised. As sensitive data might be stored, the module including the M2M UICC needs to be protected against theft and misuse.

This use case may imply specific requirements for the M2M UICC including:

- size and form factor to minimise the overall size of the mobile communication;
- size and form factor to allow automated pick and place of the MFF;
- protection against theft and misuse by e.g. M2M UICC to device pairing;

- able to operate, whilst attached in a module, withstanding normal usage vibration;
- shock resistance to withstand the forces occurring during a fall for instance;
- application interaction between M2M UICC and remote sensors.

4.18.2.2.3 Use case - Object protection

This use case is very similar to the above (persons/animal protection). Objects are equipped with portable devices containing a M2M communication module, a UICC and optionally a GPS function, which sends information automatically or on demand to a server application which can monitor the status and positioning of those objects. These services may be implemented via applications residing inside the M2M UICC.

The purpose of this application is to track and trace.

The portable devices are often placed in harsh environments. This means that they are undergoing strong vibration or even shock, extreme temperature, humidity or corrosive environments such as salt water. The connection between the M2M communication module and the M2M UICC has to withstand these elements.

The space is also very limited, meaning the size of the M2M communication module needs to be minimised, which requires also the size of the MFF to be minimised. In many cases the device shall be small enough to be hidden.

As sensitive data might be stored, the module including the M2M UICC needs to be protected against theft and misuse.

This use case may imply specific requirements for the M2M UICC including:

- size and form factor to minimise the overall size of the mobile communication;
- size and form factor to allow automated pick and place of the MFF;
- temperature and humidity according to the specific requirements of the monitoring industry;
- able to operate, whilst attached in a module, withstanding normal usage vibration;
- shock resistance to withstand the forces occurring during a fall for instance;
- designed for a product lifetime of over 10 years, taking into account a high number of read/write cycles due to frequent updates of information;
- protection against theft and misuse by e.g. M2M UICC to device pairing;
- application interaction between M2M UICC and remote sensors.

4.18.2.3 Use case - Transaction

4.18.2.3.1 Use case - PoS Terminals (Point of Sale Terminals)

Today most Point of Sales terminals are connected via a wired connection. For the use in locations like bars, restaurants, etc. this means they are mounted or placed at a fixed position, and the person who wants to perform a transaction needs to go to the location of the PoS terminal. This causes inconveniences for the sales person/waiter as well as for the customer. In the case of remote located PoS terminals, e.g. parking meters, ticketing machines, etc. these require a wired connection which is often difficult and costly to be installed and may also be exposed to damages. Another option is to connect PoS terminals via a local wireless connection which imposes some security constraints

The introduction of the M2M UICC into this environment allows additional possibilities for applications, as M2M communication modules can be installed into wireless PoS terminals, street parking and ticketing machines, etc. to provide communication for credit or debit card on-line transactions. The use of a M2M communication module incorporating a M2M UICC can offer a secure communication channel.

Typically these devices including the M2M communication module and the M2M UICC will need to pass specific security requirements for financial transactions.

This use case may imply specific requirements for the M2M UICC including:

- size and form factor to minimise the overall size of the mobile communication;
- size and form factor to allow automated pick and place of the MFF;
- able to operate, whilst attached in a module, withstanding normal usage vibration;
- protection against theft and misuse by e.g. M2M UICC to device pairing;
- secure communication over the network to a third party entity;
- application interaction between M2M UICC and remote sensors.

4.18.2.4 Use case - Control

4.18.2.4.1 Use case - Controlling vending machines

Today, vending machines are placed in various locations like e.g. inside office buildings, public buildings, public outside places, railway stations, etc. The re-filling and maintenance of vending machines is today done by dedicated personnel who have to visit the vending machines at regular intervals to check the fill-levels, re-fill the machines, perform maintenance and identify damages or malfunction.

The introduction of the M2M UICC into this environment allows additional possibilities for optimisation of the operation of vending machines. By allowing access to a mobile telecommunication network, the M2M UICC can be used by a built-in M2M communications module to provide authenticated information about the current status of the vending machine via the network to a background service. Via this connection it is possible to transmit information about the current fill-levels, maintenance status, possible damages, malfunctions, etc. Additionally it is possible to transmit updates of e.g. pricing information or perform remote maintenance via Over-The-Air functionality. This way the vending machines need only to be visited as required.

This use case may imply specific requirements for the M2M UICC including:

- temperature and humidity according to the specific requirements of the vending machine industry;
- able to operate, whilst attached in a module, withstanding normal usage vibration;
- size and form factor to minimise the overall size of the mobile communication;
- size and form factor to allow automated pick and place of the MFF;
- protection against theft and misuse by e.g. M2M UICC to device pairing;
- secure communication over the network to a third party entity;
- application interaction between M2M UICC and remote sensors.

4.18.2.4.2 Use case - Controlling production machines

Today, production machines are placed normally inside production facilities which, depending on these facilities may expose the production machine to harsh environments. The repair and maintenance of production machines is today done by dedicated personnel who have to visit the production machines at regular intervals to repair, perform maintenance and identify damages or malfunction.

The introduction of the M2M UICC into this environment allows additional possibilities for optimisation of the operation of production machines. By allowing access to a mobile telecommunication network, the M2M UICC can be used by a built-in M2M communications module to provide authenticated information about the current status of the production machine via the network to a background service. Via this connection it is possible to transmit information about the current maintenance status, possible damages which may lead to malfunctions, etc. Additionally it is possible to transmit updates of e.g. updated software or perform remote maintenance via Over-The-Air functionality. This way the production machines need only to be visited as required.

This use case may imply specific requirements for the M2M UICC including:

- temperature and humidity according to the specific requirements of the production machine industry;
- able to operate, whilst attached in a module, withstanding normal usage vibration;
- application interaction between M2M UICC and remote sensors.

4.18.3 Requirements

This clause describes the requirements on a UICC when used by Machine-to-Machine applications (M2M UICC) and requirements for an optional new form factor for M2M usage (MFF).

4.18.3.1 General M2M UICC Requirements

This clause describes requirements on all M2M UICC form factors.

Identifier	Requirement
REQ-8-18-01-01	It shall be possible to introduce different classes for the M2M UICC in order to address certain requirements from dedicated M2M segments.
REQ-8-18-01-02	Criteria for defining the different classes for the M2M UICC shall include at least form factor, temperature, humidity, vibration, shock resistance and lifetime expectation.
REQ-8-18-01-03	A mechanism shall be defined for M2M UICC to device pairing. This mechanism shall be an optional feature.

4.18.3.1.1 Specific requirements related to definition of classes

Identifier	Requirement
REQ-8-18-02-01	It shall be possible for the M2M UICC to support specific environmental conditions related to temperature as defined in TS 102 221 [1].
REQ-8-18-02-02	It shall be possible for the M2M UICC to support specific environmental conditions related to humidity as defined in TS 102 221 [1].
REQ-8-18-02-03	It shall be possible for the M2M UICC to comply to specific vibration and shock requirements resulting out of the relevant use case.
REQ-8-18-02-04	An M2M UICC shall be characterised by a set of environmental classes and a lifetime expectation.
REQ-8-18-02-05	An M2M UICC shall support a specific life time expectation based on Read/write cycles and data retention time.

4.18.3.1.2 Example for a possible class system (informative)

A possible class system for a M2M UICC may look like this:

Form Factor	Temperature	Humidity	Vibration/Shock	Lifetime expectation
F-	T-	H-	V-	L-
FA	TA	HA	VA	LA
FB	TB	HB	VB	LB
	TC	HC	VC	LC
	TD	HD	VD	LD

For example, "FA-TC-HD-VC-LA".

NOTE: It is envisaged that not all possible class combinations will exist - instead a small subset is likely.

4.18.3.2 MFF Requirements

Some M2M use cases may not be able to be realised using existing form factors for the M2M UICC. This clause details requirements for a new M2M form factor for the UICC, called MFF, that may be used for M2M uses.

Identifier	Requirement
REQ-8-18-03-01	The MFF shall be a separate hardware component.
REQ-8-18-03-02	The MFF shall be replaceable with another MFF, by using a non destructive process for both the MFF and its support (e.g. printed circuit board, or socket or connector on the circuit board).
REQ-8-18-03-03	The MFF shall be standardized in terms of physical characteristics and dimensions.
REQ-8-18-03-04	The MFF shall be able to inherit all the features specified for the UICC except the form factor.
REQ-8-18-03-05	The MFF shall provide at least the same levels of physical and logical security that the UICC provides.
REQ-8-18-03-06	The MFF shall provide means to create a constant and stable electronic connectivity to the M2M communications module.
REQ-8-18-03-07	The physical size of the MFF shall be minimised.
REQ-8-18-03-08	The MFF shall offer 8 contacts as a minimum.
REQ-8-18-03-09	The location and allocation of contacts of the MFF shall be defined.
REQ-8-18-03-10	The MFF shall use an existing industry standard package.
REQ-8-18-03-11	The package material of the UICC for M2M applications shall allow for optical personalisation.
REQ-8-18-03-12	The MFF shall be able to be connected with a connector (e.g. a socket, .etc.) to a M2M communication module (see note).
REQ-8-18-03-13	The MFF shall be able to be mechanically attached to a M2M communication module (see note).
REQ-8-18-03-14	The MFF shall allow automated pick and place for the M2M communication module manufacturing processes.
NOTE: The MFF shall fulfil both noted requirements in parallel. This means the new form factor shall be able to be used with a connector as well as to be directly mechanically attached to a M2M communication module.	

4.18.4 Interaction with existing features (informative)

Interaction with the following existing features shall be considered:

- PIN entry.
- Specific environmental conditions

4.19 Location based services for broadcast technology

4.19.1 Abstract (informative)

Location information as described in Digital Video Broadcasting systems could be made available for the UICC in order to enrich the possibilities of location based services. This clause lists the corresponding usecases and requirements.

4.19.2 Use Cases (informative)

Various type of Digital Video Broadcasting technologies are under deployment, such as DVB-H, DVB-T; DVB-SH or T-DMB. Whatever is the broadcasting technology, the location information is available in the Terminal receiving the broadcasted flow. It could be beneficial for the UICC to be able to retrieve the location information which is available for this broadcasted flow. Today OMA BCAST 1.0 specification [i.4] already mentions a service called "Black Out" which allows location based access restriction, which is used for restricting specific content such as baseball programme when the end user is located closed to the stadium where the baseball game is actually happening. In a more general way, segmented broadcasted content could be made available to the end user, depending on its location. Giving access to the UICC to such information, could allow to implement those services inside the UICC.

4.19.3 Requirement for retrieving location information for broadcast technology

REQ-8-19-01-01	There shall be a mechanism allowing the UICC to request location information, based on broadcasting technology such as DVB-H, DVB-T; DVB-SH or T-DMB.
REQ-8-19-01-02	The information transmitted to the UICC shall be compliant with the DVB format as described in EN 300 468 [11] and EN 302 304 [12]
REQ-8-19-01-03	There shall be a discovery mechanism allowing the UICC and the Terminal to exchange their support of such mechanism.

4.19.4 Interaction with existing features (informative)

(none).

4.20 Terminals with reduced functionality

4.20.1 Abstract (informative)

TS 102 223 [2] currently assumes that all terminals provide a keyboard, display, alerting, multiple languages and ability to provide speech calls. Certain terminals, used in connection with various applications such as M2M, have reduced or restricted functionality. In these cases, they often lack common input or output components or possibilities.

4.20.2 Use case (informative)

4.20.2.1 Use case - Data card

The data card is a good example of a terminal without some more common input or output functionality. In particular, a data card is missing both a display and a keypad; and it normally does not allow speech calls. Nevertheless, it is in the interest of data card manufacturers, vendors and users to be able to guarantee interoperability through type approval. A mechanism that provided information to the UICC about such restrictions on terminal functionality would allow type approval to be systematically adapted to those restrictions.

4.20.3 Requirements

This clause describes the requirements on a terminal for providing functionality information about their reduced capabilities.

Identifier	Requirement
REQ-8-20-01-01	A mechanism to identify the missing capabilities of terminals with reduced functionality (e.g. no display, no keyboard, no speech calls, no alerting, no multiple languages) to the UICC and the respective impact on CAT commands shall be defined.
REQ-8-20-01-02	The terminal behaviour in response to CAT commands shall be specified in a way that minimises impact on existing applications (e.g. by ignoring alpha identifiers that inform the subscriber about a command on terminals without a display).

4.20.4 Interaction with existing features (informative)

The purpose of these requirements are to provide a mechanism to avoid invalid assumptions about existing features or functionality. An interaction with these features is not foreseen.

4.21 Digital Rights Management

4.21.1 Abstract (informative)

This clause describes usecases and requirements to add the ability for the UICC to store digital rights and for the terminal to manage them according to the OMA SRM specifications.

The OMA SRM specification details the management procedures and the digital rights definitions. These requirements extend the SRM capabilities to the UICC.

4.21.2 Use cases (informative)

This clause describes the use cases for digital rights management and storage on the UICC.

4.21.2.1 Use case - Transfer of protected contents and rights by using a UICC

A user, who has collected several DRM-protected contents in an old mobile device, decides to buy a new device.

When the user has the new device, he would like to play all his content in it, and therefore, transfers the content and/or rights from the old device to the new one using a UICC.

To do that:

1) The DRM Agent in the user's old device transfers the content and/or rights from the old device to the UICC after a successful mutual authentication.

2) The DRM content and/or rights stored on the card are transferred from the card to the user's new device after a successful authentication between both entities.

3) The user can consume the content acquired with the old device in the new one.

The same steps have to be followed to share content among devices that may belong to different users and that may be of different types (e.g. mobile phone, PC, etc.).

4.21.2.2 Use case - Provisioning of rights in the UICC

A user, who is subscribed to some services that a Network Service Provider offers, uses the UICC to store the acquired rights and his account details.

The user decides to buy a new device and wants to continue playing the same services by only plugging his UICC in the new device and performing the actions he used to do: surf to the portal, choose the content, download it, pay for the transaction and play it.

To do that:

1) The user downloads rights that are installed directly in his UICC (the rights can be uploaded from the UICC to the device or consumed directly on the UICC.

2) The user can consume the content associates with the rights in any device containing the UICC.

4.21.2.3 Use case - Direct rendering of DRM-protected content by using the UICC

A user wants to play DRM-protected content stored in his UICC without transferring the content and rights to the rendering device (he does not own the device, the device has not enough free space, etc.).

This scenario is possible only after a successful authentication between the card and the rendering device.

4.21.2.4 Use case - Pre-loading of rights by using the UICC

A Service Provider is providing services when users purchase a new network subscription to, for example, attract new subscriber by promoting free and DRM content.

The Service Provider provisions DRM-protected content on the mobile phone or a removable media if available (e.g. MMC, Smart Card …), and the corresponding set of Rights is installed in the UICC at the factory during the personalization.

If the user subscribes to this new service, he will enjoy the content just by putting the UICC into the handset and switching on the device, without any network interaction.

4.21.3 Requirements

This clause describes the requirements on the UICC that allows it to have digital rights stored and managed.

Identifier	Requirement
REQ-8-21-01-01	There shall be a secure mechanism to allow the DRM agent in the terminal to retrieve rights from the UICC according to the OMA SRM specifications [14] and [15].
REQ-8-21-01-02	There shall be a secure mechanism to allow the DRM agent residing in the terminal to write, remove, and update rights on the UICC, according to the OMA SRM specifications [14] and [15].
REQ-8-21-01-03	There shall be a secure mechanism to allow the DRM agent residing in the terminal to use rights which are transferred from the UICC, according to the OMA SRM specifications [14] and [15].
REQ-8-21-01-04	There shall be a secure mechanism to allow the DRM agent residing in the terminal to use rights that are stored in the UICC and update state information in the UICC for stateful rights, according to the OMA SRM specifications [14] and [15].
REQ-8-21-01-05	There shall be a recovery procedure for unexpected communication interrupt between the UICC and the DRM agent residing in the terminal, according to the OMA SRM specifications [14] and [15].
REQ-8-21-01-06	Both the terminal and UICC shall be able to action revocation information from the rights server, according to the OMA SRM specifications [14] and [15].

4.21.4 Interaction with existing features (informative)

(none).

Annex A (informative): Requirement numbering scheme

This annex summarizes the decision made at ETSI SCP #26 on how to standardize requirements from Release 8 onwards.

In this scheme Release 8 of the present document will contain all the new requirements starting with Release 7.

NOTE: The requirements numbering scheme already includes an indication of the release for which each requirement is introduced.

The numbering of requirements will not be altered if a requirement is made void. When additional requirements are added to an existing set of requirements the "last digit" of the new requirement will be consecutive from the existing requirement.

To clarify how this can be achieved and how different types of change should be presented, examples are given below.

EXAMPLE 1: A new requirement.

Identifier	Requirement
REQ-7-0X-0Y-01	The UICC shall ……
REQ-8-0X-0Y-02	The UICC shall not be ……

- A new feature will have its own new clause.
- Additions to existing use cases or requirements will be added to the existing clause.

EXAMPLE 2: Modification of a Release 7 requirement for Release 8.

This example is when the original Release 7 requirement is unmodified at Release 7 but changed for Release 8.

Identifier	Requirement
REQ-7-04-05-02	The UICC shall ……
REQ-8-04-05-03	The UICC shall ……
REQ-7-04-05-04	The UICC shall ……

- The Release 7 requirement is replaced by the modified content and now becomes a Release 8 requirement.

EXAMPLE 3: Essential correction to a Release 7 requirement.

This example is when an earlier release of the present document is changed due to an essential correction.

Identifier	Requirement
REQ-7-04-05-03	The UICC shall ……
REQ-7-04-05-04	The UICC shall ……

- The later releases of the present document are changed to accurately reflect the changes of the earlier releases. (The changes in this example still show as being Release 7 requirements).

Annex B (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	Old Version	CR	REV	CAT	SUBJECT	Resulting Version
SCP-22	SCP-050304	2.1.0					7.0.0
	SCP-050306	7.0.0	001		B	Requirement for Secure channel between the UICC and a terminal end point	7.1.0
SCP-23	SCP-050467	7.1.0	004		B	Introduction of a mechanism to perform authenticate command longer than 255 bytes	7.2.0
			006		B	Requirement for new CAT mechanisms to indicate the bearer connection status	
			007		B	Introduction of a New UICC-Terminal interface	
	SCP-050514		008		B	Power supply indication mechanism by the terminal	
	SCP-050515		002		B	Terminal network connectivity for a UICC based application acting as a server	
	SCP-050517		005		B	API for registration of applications to a Smart Card Web Server and for Data Exchange with a Smart Card Web Server	
	SCP-050526		003	2	B	Requirements for specific UICC environmental conditions	
	SCP-050530		009		B	Introduction of high density memory capability for UICC	
SCP-24	SCP-060031	7.2.0	010		D	Clean up of the abbreviations clause	7.3.0
SCP-25	SCP-060115	7.3.0	011		B	CR for UICC Internet connectivity	7.4.0
	SCP-060161		012	1	B	Requirement for Contactless UICC Services	
SCP-26	SCP-060263	7.4.0	013		C	Modification of the optional relative humidity requirement in the Specific UICC environmental conditions Requirement	7.5.0
	SCP-060293		014		C	Proposal to complete the secure channel requirements	
	SCP-060295		015		D	Recommended working procedure for requirements in Release 8 (onwards)	
SCP-27	SCP-060454	7.5.0	016		D	Clarification of secure channels interaction with logical channels	7.6.0
		7.6.0				Editorial correction spotted during REQ#12	7.6.1
	SCP-070071	7.6.1	018		B	Address naming for IP connectivity	7.7.0
	SCP-070072		017		C	Updated requirements for the Launch Application feature	
SCP-31	SCP-070284	7.7.0	020		B	Naming for IP Connectivity	7.8.0
SCP-33	SCP-070444	7.8.0	021	1	B	Association of an SCWS application with a URI	8.0.0
SCP-35	SCP-080050	8.0.0	022	1	B	Addition of requirements for Confidential Applications (clause 4.17)	8.1.0
SCP-38	SCP-080370	8.1.0	023	1	B	Allow applications registered to the SCWS to issue proactive commands	8.2.0
SCP-38	SCP-080369	8.1.0	024		B	Trusted Service Manager usecase and requirements in Confidential Applications	8.2.0
SCP-39	SCP-080451	8.2.0	025	1	B	Requirements for a UICC for M2M (machine-to-machine) applications	8.3.0
SCP-39	SCP-080455	8.2.0	028	1	B	Introduction of DVB location information usecases and requirements	8.3.0
SCP-39	SCP-080479	8.2.0	029	1	F	Clarification of availability of proactive handler for SCWS applications	8.3.0
SCP-39	SCP-080456	8.2.0	030	1	B	Requirements for the identification of terminals with reduced functionality	8.3.0
SCP-39	SCP-080476	8.2.0	031		B	Addition of Secure Removable Media on UICC requirements (renumbered from 24r2 to 31)	8.3.0
SCP-40	SCP-090056	8.3.0	032		F	Correction of requirements for Confidential Applications	8.4.0
SCP-41	SCP-090154	8.3.0	034		F	Modification of requirement REQ-8-17-04-05 to remove method level access policy for Third Party Applications	8.4.0

History

Document history		
V8.0.0	January 2008	Publication
V8.1.0	May 2008	Publication
V8.2.0	October 2008	Publication
V8.3.0	January 2009	Publication
V8.4.0	June 2009	Publication