ETSI TS 102 412 V16.0.0 (2020-07)

TECHNICAL SPECIFICATION

Smart Cards;
Smart Card Platform Requirements Stage 1
(Release 16)

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

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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 (https://ipr.etsi.org/).

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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

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.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

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

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

- 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.

Referenced documents which are not found to be publicly available in the expected location might be found at https://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.

The following referenced documents are necessary for the application of the present document.

[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); LTE; Characteristics of the Universal Subscriber Identity Module (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".

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

[16]   ETSI TS 102 241: "Smart Cards; UICC Application Programming Interface (UICC API) for Java Card (TM) (Release 8)".

[17]   ETSI TS 127 007: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; AT command set for User Equipment (UE) (3GPP TS 27.007 Release 9)".

[18]   ETSI TS 102 613: "Smart Cards; UICC - Contactless Front-end (CLF) Interface; Physical and data link layer characteristics".

[19]   ETSI TS 102 622: "Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI)".

[20]   ISO/IEC 18000 (all parts): "Information technology -- Radio frequency identification for item management".

[21]   ETSI TS 102 483: "Smart cards; UICC-Terminal interface; Internet Protocol connectivity between UICC and terminal (Release 8)".

[22]   IETF RFC 2616: "Hypertext Transfer Protocol -- HTTP/1.1".

[23]   ETSI TS 102 484: "Smart Cards; Secure channel between a UICC and an end-point terminal".

[24]   ETSI TS 102 600: "Smart Cards; UICC-Terminal interface; Characteristics of the USB interface".

[25]   ETSI TS 102 671: "Smart Cards; Machine to Machine UICC; Physical and logical characteristics".

[26]   GlobalPlatform: "Requirements for NFC Mobile: Management of Multiple Contactless Secure Elements v2.0".

[27]   NFC Forum: "NFC Controller Interface (NCI) Technical Specification Version 1.1".

[28]   IEEE Standard for Low-Rate Wireless Networks (IEEE 802.15.4-2015).

[29]   IEEE Standard for Low-Rate Wireless Networks - Amendment: Enhanced Ultra WideBand (UWB) Physical Layers (PHYs) and Associated Ranging Techniques (draft IEEE 802.15.4z).

2.2   Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

- 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.

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[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".

[i.5]   Mobile Broadband in Notebooks Guidelines, version 4.0, December 2009.

[i.6]   ETSI TR 102 906: "Smart Cards; UICC-Terminal interface; UICC in Mobile Broadband Notebook".

[i.7]   ETSI TR 131 970: "Universal Mobile Telecommunications System (UMTS); LTE; 5G; UICC power optimisation for Machine-Type Communication (3GPP TR 131 970)".

3   Definition of terms, symbols and abbreviations

3.1   Terms

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

AT command interface: modem interface protocol specified in ETSI TS 127 007 [17]

card emulation mode: mode of operation where the UICC emulates a contactless card through the CLF

central repository: repository of registered applications residing in the UICC

chunked transfer-coding: mechanism that allows HTTP messages to be split in several parts as defined in IETF RFC 2616 [22]

ContactLess Front-end (CLF): circuitry in the terminal which:

- Handles the analog part of the contactless communication.

- May handle some layers of the contactless protocol.

- May exchange data with the terminal and the UICC.

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

CLFI Protocol (CLFIP): 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-SRM Agent Mutual Authentication: DRM Agent and the SRM Agent can authenticate each other based on credentials that are securely provisioned in each

NOTE: 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].

external entity: entity that is external to the UICC and the modem; it can be the Mobile Broadband Notebook or a distant entity (e.g. a server)

HCI Host: logical entity that operates one or more contactless service(s), as defined in ETSI TS 102 622 [19]

High Speed Protocol (HSP): running on top of the NUT interface

Host Controller Interface (HCI): HCI is a part of the implementation of CLFIP, as defined in ETSI TS 102 622 [19]

M2M communication module: electronics system including all necessary components to establish wireless communications between machines

NOTE: M2M communication modules are usually integrated directly into target devices, such as Automated Meter Readers (AMRs), vending machines, alarm systems, car equipment or others.

M2M device applications: applications deployed on a machine to machine device that deliver a service to the UICC

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

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

Managing Host: HCI Host which is in charge of resolving conflicts and interoperability issues between different contactless applications provided by different hosts

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

Mobile Broadband: Mobile Network Operator (MNO) service that provides access to the Internet via the MNO's cellular network

> NOTE: The service is available to mobile phones or to computers. Mobile Broadband is not limited to just a 3G network but also to any future network bearer or services defined by 3GPP or 3GPP2, e.g. Long Term Evolution (LTE).

Mobile Broadband Notebook: portable personal computer equipped with, or connected to, a cellular modem and a UICC hosting a Network Access Application and supporting Mobile Broadband

modem: terminal that has a modem interface (such as an AT command interface)

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.

partition: logical separation of UICC memory

peer to peer mode: mode of operation in which two systems, one of them may be composed of a UICC and a terminal, interact as equal peers with no master and slave roles and where either system may initiate communications

reader mode: mode of operation in which a UICC along with a CLF behaves as a contactless smartcard reader

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 (SRM): 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[TM] earpiece connected to a Mobile Terminal.
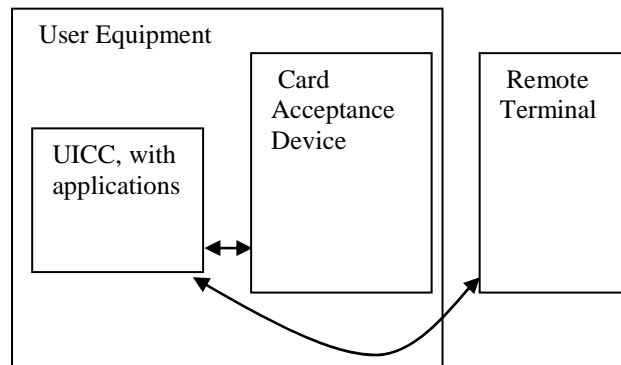
Figure 1: Possible secure channels with a UICC

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.

Ultra Wideband: radio technology using a large portion of the radio spectrum which physical and MAC layer are defined by IEEE 802.15.4 specifications [28]

Ultra Wideband Controller (UWBC): circuitry in the terminal which acts as a front end to the UWB transceiver

unsolicited result code: mechanism defined for the AT command interface that allows the modem to indicate an event (defined in ETSI TS 127 007 [17])

3.2 Symbols

Void.

3.3 Abbreviations

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

3GPP   3rd Generation Partnership Project

4FF	Fourth UICC form factor
ADF	Application Dedicated File
AEC	Automotive Electronics Council
AID	Application IDentifier
AMR	Automated Meter Reader
APDU	Application Protocol Data Unit
API	Application Programming Interface
APN	Access Point Name
AT	ATtention
BCAST	BroadCAST
BIP	Bearer Independent Protocol
CAD	Card Acceptance Device
CAS	Conditional Access System
CAT	Card Application Toolkit
CAT-TP	Card Application Toolkit - Transport Protocol
CD	Compact Disc
CEK	Content Encryption Key
CLF	ContactLess Front-end
CLFI	ContactLess Front-end Interface
CLFIP	ContactLess Front-end Interface Protocol
CPU	Central Processing Unit
CSIM	CDMA Subscriber Identity Module
DF	Dedicated File
DM	Device Management
DMB	Digital Media Broadcasting
DNS	Domain Name System
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
EEM	Ethernet Emulation Model
EF	Elementary File
EMV®	Europay Mastercard Visa
EPC	Electronic Product Code
EPCGlobal	Electronic Product Code Global
ESN	Electronic Serial Number
FFS	For Further Study
FLO	Forward Link Only
FTP	File Transfer Protocol
GBA	Generic Bootstrapping Architecture
GPRS	General Packet Radio Service
GPS	Global Positioning System
GSM	Global System for Mobile communications
GSMA	GSM Association
HCI	Host Controller Interface
HSP	High Speed Protocol
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	Secure HyperText Transfer Protocol
ICC	Integrated Circuit Card
ICCD	Integrated Circuit Card Device
ICCID	Integrated Circuit Card IDentifier
IMEI	International Mobile Equipment Identity
IMS	IP Multimedia Services
IP	Internet Protocol
IPSEC	Internet Protocol SECurity
ISIM	IP Multimedia Services Identity Module
ISO	International Organization for Standardization

IT	Information Technology
JSR	Java^{TM} Specification Request
LAC	Location Area Code
LAN	Local Area Network
LTE	Long Term Evolution
M2M	Machine to Machine (communication)
MBMS	Multimedia Broadcast/Multicast Service
MBNB	Mobile Broadband NoteBook
MCC	Mobile Country Code
ME	Mobile Equipment
MFF	Machine to Machine Form Factor
MMC	MultiMediaCard
MMI	Man Machine Interface
MMS	Multimedia Messaging Service
MNC	Mobile Network Code
MNO	Mobile Network Operator
MO	(Device) Management Object
MT	Mobile Termination
MVNO	Mobile Virtual Network Operator
NAA	Network Access Application
NCI	NFC Controller Interface
ND	No Display
NFC	Near Field Communication
NMR	Network Measurement Results
NUT	New UICC-Terminal
OMA	Open Mobile Alliance
OTA	Over The Air
P2P	Peer to Peer
PC	Personal Computer
PDA	Personal Digital Assistant
PIN	Personal Identification Number
PKI	Public Key Infrastructure
POP	Post Office Protocol
POS	Point Of Sale
PPAP	Production Part Approval Process
PPSE	Proximity Payment System Environment
PSK	Pre-Shared Key
RAM	Remote Application Management
RCS	Rich Communications Services
REQ	REQuirement
RF	Radio Frequency
RFID	Radio Frequency Identification
RO	Rights Object
RTP	Reliable Transport Protocol
SC	Smart Card
SCWS	Smart Card Web Server
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SM	Short Message
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SRM	Secure Removable Media
SWP	Single Wire Protocol
TCG	Trusted Computing Group
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
T-DMB	Terrestrial - Digital Multimedia Broadcasting
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TMP	Trusted Media Player
TSM	Trusted Service Manager
TV	TeleVision

UA	(Digital Rights Management) User Agent
UDP	Datagram Protocol
UE	User Equipment
UI	User Interface
UWB	Ultra Wideband
UWBC	Ultra Wideband Controller
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USB EEM	Universal Serial Bus Ethernet Emulation Model
USB ICCD	Universal Serial Bus Integrated Circuit Card Devices
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
USSM	UICC Security Service Module
WAP	Wireless Application Protocol
WIM	Wireless Identity Module
WLAN	Wireless Local Area Network
XML	eXtensible Markup Language

4 Requirements

4.0 General

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;

- Multicast dataflow in UICC;

- New type of data storage and access;

- CAT access over a modem interface;

- Applications and services over USB;

- Integration of a UICC in a Mobile Broadband Notebook;

- Fourth UICC Form Factor;

- Name resolution mechanism for the UICC;

- UICC access optimization.

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 ETSI 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 (ETSI 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 ETSI 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 ETSI TS 151 011 [4] with that of a USIM in ETSI 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)

ETSI 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 will 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)

4.5.2.0 General

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 is going 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 it will be assumed that 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, use cases linked with User Interface, Device Management (DM), Digital Right Management (DRM) are covered.

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 the communication between the UICC and the terminal is focused on;

- the information flowing from the card to the terminal; and

- vice versa, is in plain text [2].

In this respect, the two cases can be considered 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.
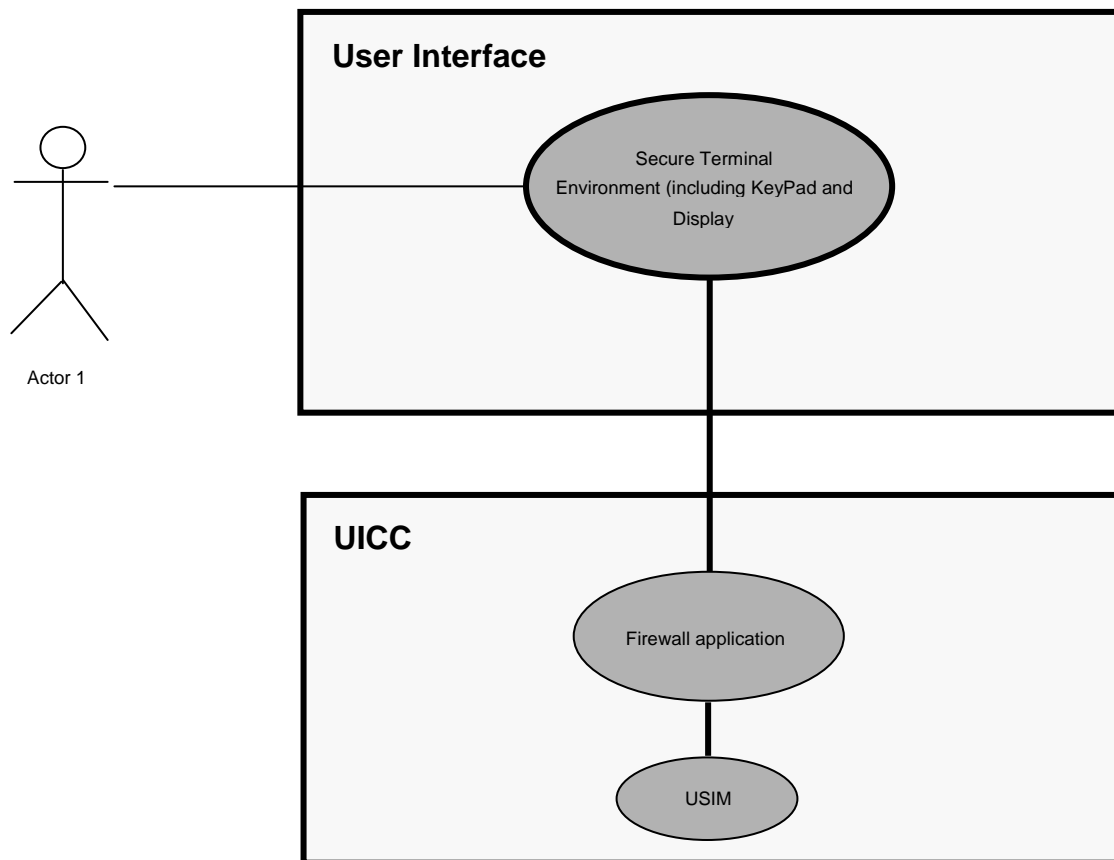
Figure 2: User Interfaces

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) will 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.
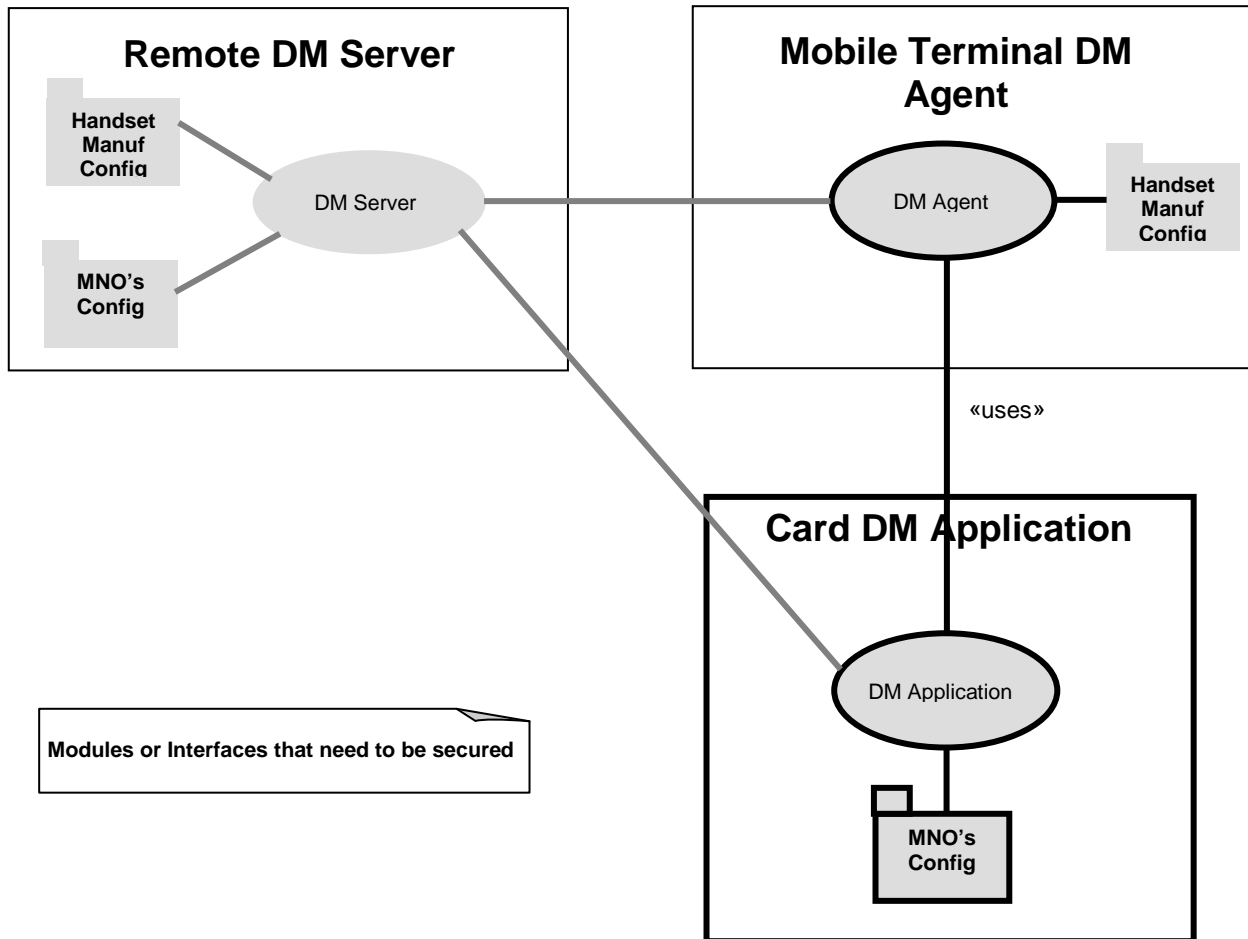
Figure 3: Device Management (DM)

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.
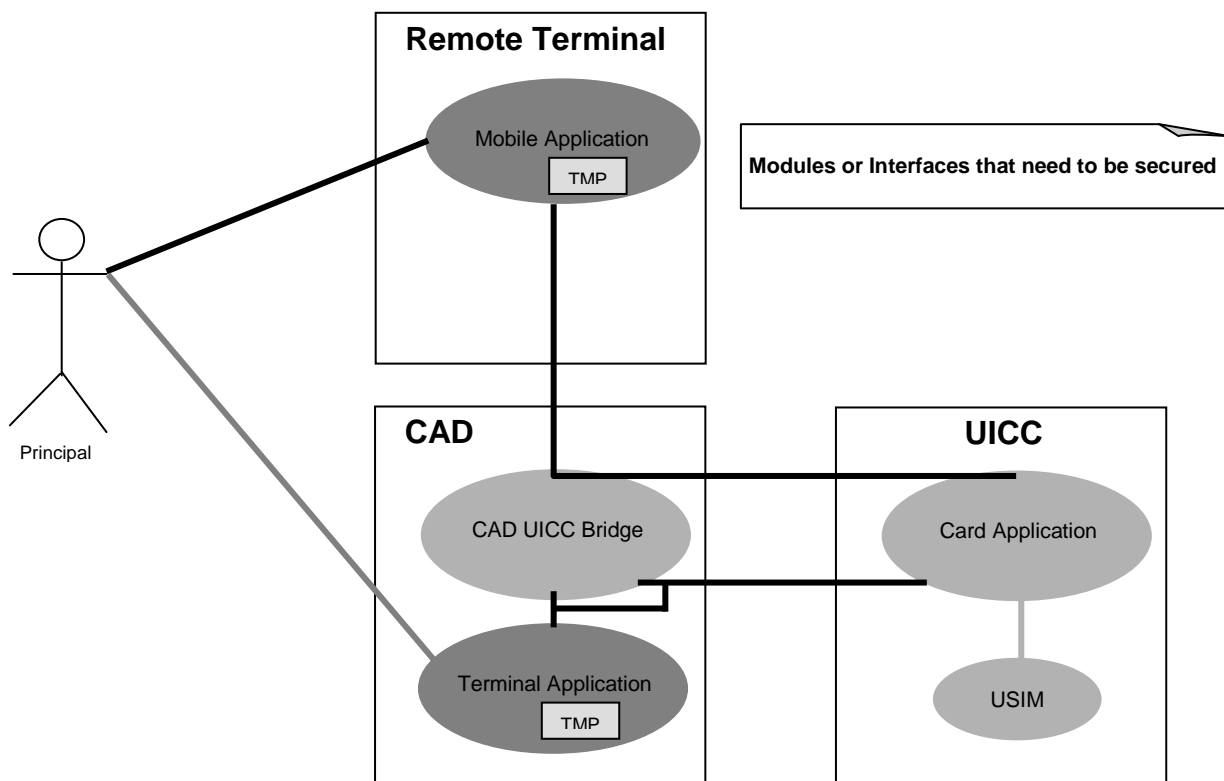
Figure 4: Distributed application

4.5.2.4 Use case - Toolkit commands protection

Applications residing in the UICC using Card Application Toolkit (either events or proactive commands) may transmit some sensitive data, such as secret code value or personal information. To avoid man-in-the-middle attacks, there is a need to transfer toolkit commands via a dedicated secure channel.

Because the data carried by SEND DATA and RECEIVE DATA could be large and could be protected by another mechanism (e.g. HTTPS), the possibility to exclude SEND DATA and RECEIVE DATA has to be considered in this toolkit dedicated secure channel.

4.5.3 Requirements

4.5.3.0 General

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.
REQ-10-05-01-06	There shall be a mechanism defined to protect all toolkit-related traffic for all toolkit applications as described in ETSI TS 102 223 [2], by means of a dedicated secure channel.
REQ-10-05-01-07	There shall be a secured mechanism allowing the UICC to indicate to the terminal exclusion or inclusion of SEND DATA and RECEIVE DATA from this protection mechanism.
REQ-10-05-01-08	The exclusion or inclusion of the SEND DATA and RECEIVE DATA from/in this protection mechanism shall be defined at bearer level (e.g. SEND DATA and RECEIVE DATA for local bearer may be protected while SEND DATA and RECEIVE DATA for remote bearer may not be protected).
REQ-10-05-01-09	There shall be a mechanism that allows the UICC to enable/disable the use of this protection mechanism for the toolkit traffic and to inform the Terminal accordingly.
REQ-10-05-01-10	There shall be an API to enable an application to request the use of this protection mechanism for the toolkit traffic.
REQ-10-05-01-11	There shall be an API to enable an application to indicate that the use of this protection mechanism for the toolkit traffic is no longer needed.
REQ-10-05-01-12	If at least one CAT application requests this protection mechanism, the UICC shall enable this protection mechanism.
REQ-10-05-01-13	The UICC shall disable this protection mechanism when no more CAT applications are requesting to use this protection mechanism.
REQ-10-05-01-14	For this protection mechanism there shall be a mechanism to apply "integrity without confidentiality", "confidentiality without integrity", or "confidentiality and integrity".

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.

4.5.4.2 CAT access over a modem interface

CAT access over a modem interface also has requirements to protect toolkit related traffic. To reduce the proliferation of mechanisms to secure CAT related functionality, the mechanisms could be aligned.

4.6 Authenticate command longer than 255 bytes

4.6.1 Abstract (informative)

ETSI TS 102 221 [1] specifies only a short length for commands and, therefore large amount of data is 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 is 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 ETSI 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 will 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^{TM} 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 will be revised and New UICC-Terminal interfaces will 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 will 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)

4.8.2.0 General

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 (NUT) 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-Release 7-commands, the default UICC power shall not exceed what is specified in ETSI 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 ETSI 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 ETSI 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.

To enable a seamless graphical user interface, an entry page of the Smart Card Web Server can be reached directly from a terminal icon in addition to the one representing the UICC CAT based services.

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, etc.).
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.
REQ-9-09-01-07	A mechanism shall be provided that allows access to the Smart Card Web Server directly from the terminal's icon/menu item representing the UICC (Smart Card Web Server) based services (menu title), without the need of taking the additional step of selecting one of the CAT menu entries.
REQ-9-09-01-08	This mechanism shall be available in addition to the CAT menu.
REQ-9-09-01-09	A mechanism shall be provided that enables the UICC to retrieve information about terminal capabilities (e.g. size, colour depth) regarding an icon that the UICC can provide to the terminal for the menu title.

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)

4.10.2.0 General

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.
REQ-10-10-01-08	There shall be a mechanism to allow a Java Card Applet to access the message body of a HTTP request which exceeds the UICC buffer size, e.g. when such a HTTP request uses chunked transfer-coding.

4.10.4　Interaction with existing features (informative)

Starting with Release 10, the mechanism for accessing the message body of a HTTP request exceeding the UICC buffer will most likely require an indication allowing applications to differentiate between this mechanism's behaviour and the behaviour specified by previous releases.

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)

4.11.2.0　General

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 ETSI 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-Release 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-Release 7 (ETSI TS 102 221 [1], Release 6) 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 ETSI 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 will 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 ETSI TS 102 221 [1], table 6.4) up to the maximum (see ETSI 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 ETSI TS 102 221 [1], table 6.4 (but still within the range defined in ETSI 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 ETSI 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 will 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)

4.14.2.0 General

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 will 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 is 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)

4.15.2.0 General

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).

In addition, a large portion of contactless access systems is based on ISO/IEC 15693 [10]. The user carries a device (RFID tag) in order to get access to specific areas. In existing ISO/IEC 15693 [10] based access systems, an identification code is provided by the RFID tag. In a terminal, the RFID tag is emulated and the UICC - as a secure element - handles the usage (e.g. the lifetime cycle) of the identification code.

One example of ISO/IEC 15693 [10] based technology is used with ski lifts. The RFID tags are read over distances (i.e. a few tens of centimetres) so that an individual passing a gate is freed from any explicit actions, e.g. putting the tag in front of a tag reader. The features of such RFID tags are emulated by the terminal and the background system handles the lifetime status of the identification codes using the UICC as a secure element.

The terminal may also be used in reader mode. It is used by the person managing the access or the vendor of the tags to read from and write access rights related data to the tags (renew or grant access rights to the tags).

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).

For the case where the terminal emulates a tag as defined in ISO/IEC 15693 [10], the UICC stores a unique identifier of the user which is then used to grant or deny access rights. Renewal of the access rights (e.g. ski pass) is made secure and easier since the UICC can be remotely accessed. This application may be linked to a payment application.

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 will 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.

For the case where the terminal operates as a reader as defined in ISO/IEC 15693 [10], the access rights management is hosted in the UICC since this management involves very sensitive data and functions which requires a high level of security. UICC applications which manage the access rights may require interaction with other parts of the access infrastructure (e.g. getting remote access to a server).

4.15.2.2 Use case - Tickets

4.15.2.2.0 General

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^{TM} MiFare^{TM}, FeliCa^{TM}, 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 is providing 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.

P2P Case:

d) Flight ticket management - On arrival at the airport, check-in is performed at the automatic kiosk. The UICC is used to authenticate the user at the kiosk. After authentication, the electronic ticket is transferred to the UICC and will be used later for access control to the plane. At the same time, the passenger's agenda is updated on his mobile terminal with information related to his flights. This information will be available even when the mobile terminal is deactivated (no RF: plane mode) for the take-off time. 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 telecommunications 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:

- Implementation of the EMV® PPSE application: The PPSE application manages two lists of payment applications, one list with applications requiring the availability of the Device User Interface and one with applications that do not have such a constraint. Depending on the availability of the User Interface on the device, the PPSE application will disclose one list or the other. To do so, a mechanism is needed for the PPSE to retrieve the current state of the User Interface (including the screen, the keyboard or the touchscreen).

- Transaction requiring to display information mandating an interaction with the end user (e.g. display of an amount): The user taps their mobile at the contactless terminal. Once triggered, the contactless application checks that the display is available. If the display is not available, the transaction cannot be performed and the contactless application closes or rejects the transaction immediately. However, if the display is available, the contactless application can move forward with the transaction.

- Higher payment transaction amount if PIN entry is possible: The user taps their mobile at the contactless terminal and the amount of the transaction requires the user to enter a PIN. Once triggered, the contactless application checks that the display AND the touchpad are available. If the display OR the touchpad is not available, the transaction cannot be performed and the contactless application closes or rejects the transaction immediately. If the display AND the touchpad are available, the contactless application can move forward with the transaction.

Depending on the policy set by the payment application running on the UICC, a confirmation of the payment by the end user may be required. This confirmation can be performed by a PIN entry from the end user on the terminal. As payment associations may require the management of the PIN in a secure environment, the use of a TEE (Trusted Execution Environment) in the terminal may be mandatory. With this use case, communication between the application running on the TEE and the application running on the UICC is required but in some terminals, there is no interface between the TEE and API in charge of managing the modem and the UICC. However, an interface is available between the TEE and the CLF. In order to allow flexible and efficient implementation in the terminal, communication with the UICC over HCI is a possible solution.

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.

P2P mode:

- Movie theatre - A user enters a movie theatre, pays with his mobile terminal (Contactless payment based on UICC), receives a free ticket to exit the parking lot (Ticketing), receives a synopsis of the movie and his mobile terminal is automatically switched to silent mode. By using the P2P mode, the transaction will be faster and will not require switching between card emulation and reader mode. The different aspects (payment, ticketing, advertisement, etc.) may be provided by one or more applications.

- Railways - A user does not validate his ticket loaded in his mobile phone while entering the train. During travel, a railways employee asks the user to provide evidence regarding travel payment (the electronic ticket). The user's terminal battery is empty. In this situation, the "not battery powered" mode of operation is needed in order to avoid fraud. This mode is also needed if validation of the transport pass is required on the exit gate in order to calculate fare rate.

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.

P2P mode:

- During the payment for an item, the loyalty application is activated at the same time in order to credit the transaction to the loyalty program. As a result of the transaction, the invoice will show the amount of the transaction, the discount obtained thanks to the loyalty program and the new status of the loyalty program. By operating the two independent applications in parallel, the RF channel usage is optimized and the user experience is improved. These two applications may be located in two different hosts of the system (e.g. UICC for the payment application and Terminal for the loyalty application) because they have different security requirements and different issuers.

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.

4.15.2.7 Use case - Retail

4.15.2.7.1 System aspects of the use case

RFID is an efficient solution to identify objects and items (e.g. with an EPCGlobal code) in the delivery chain and to handle information about these objects. In logistic applications, delivered items can be checked against the delivery documents, which may be electronically transmitted and the confirmation of the reception of the delivered item can be provided by the UICC. The comparison process may be run by the UICC. This approach benefits from the secure environment provided by the UICC, giving an unambiguous proof of receipt.

4.15.2.7.2 UICC role in the use case

The UICC operates in reader mode:

a) Retail shop operator: An application residing in the UICC reads the tag attached to a parcel and sends a signed proof of receipt.

b) Delivery man: An application residing in the UICC reads the tag attached to the parcel in order to keep track of the delivery.

In this scenario, the UICC application may add the location and the time-stamp information. Such UICC applications may require interaction with other parts of the delivery system (e.g. remotely accessing a server).

4.15.2.8 Consideration about multiple applications in peer to peer mode

4.15.2.8.1 System aspects of multiple applications in peer to peer mode

Peer to peer operation represents a future evolution of contactless communications in the Contactless Communications area. Peer to peer can offer true multiapplication support due to not being based on legacy 'one card - one application' principles. Contactless modes of operation using card emulation mode and reader mode typically requires that only one UICC application is activated for each technology (e.g. Type A or type B) because the reader expects a single, mono-application card. This leads to a situation where a user may have multiple contactless applications, for example a payment application, a rail travel application, a bus travel application and an access control application but needs to actively select which application to 'activate' before presenting his mobile device to an external reader. This can degrade the users experience and cause unnecessary delays and frustration at the point of use.

By implementing a method of efficient connections for these multiple applications the user experience and technology acceptance could be improved.

Multiple applications may run from multiple active hosts (e.g. terminal and UICC).

4.15.2.8.2 Service discovery in peer to peer mode

A terminal may use a peer to peer contactless mode in addition to the existing modes of operation which would also include one or multiple discovery services. These discovery services would allow a peer device to see what service identifiers are available in the other peer device in order to allow the missing applications providing these services to be provisioned according to host policy. Furthermore, peer to peer mode typically allows for more than one logical communication channel so more than one application may be communicating with an external device at the same time.

4.15.2.8.3 Application connection in peer to peer mode

Only the applications having their counterpart in the peer can work. Therefore, the terminal and the peer device may try to connect the applications without previously using service discovery.

4.15.2.8.4 Customer care in peer to peer mode

In multi-host environments, it may be that the hosts (and relevant P2P applications) are not all supported by the same service provider. For example the terminal might perform P2P applications provided by a service provider while the UICC performs other P2P applications provided by the mobile network operator.

In such an environment, each service provider should be responsible only for the services it supports.

At present, in case of a problem or question related to a mobile application (whether in the terminal or in the UICC), the end user will always apply to the MNO's customer care service.

In multi-host environments, it is important that the end user can identify which peer to peer services he is using, so that he can call the correct customer care and get the right answer without wasting time and money.

The new features brought by P2P may cause more frequent calls to customer care. For example, conflicting or incompatible applications running in different hosts may bring new issues to the end user. In order to minimize these issues, conflicts and incompatibilities management may be delegated to one host in charge of solving these issues. This process may imply end-user interaction or may be automated in a host.

4.15.2.9 Considerations about the P2P technology

P2P mode may solve several deployment issues and help several use cases:

- Evolution of RF protocols: a user inserts his UICC containing some P2P applications in a new terminal supporting a new P2P RF standard (e.g. based on ISO/IEC 14443 [8] Very High Data Rate technology), allowing faster communications. The user operates the previous use cases without any upgrade of the UICC applications and/or the UICC.

- Application deployment: A new P2P application deployed into a user's terminal using OTA will be available immediately and will not interfere with any under layer parameters of already installed applications.

- Multi host environment: P2P applications may be deployed using several hosts. For example, secure applications may be deployed in the UICC or in a secure element of the terminal. Applications like Bluetooth^{TM} pairing, URL exchange may be addressed directly by the terminal. All these applications may be used simultaneously and independently of the device architecture and the location where the applications are running.

- RF technologies conflict management: The legacy infrastructure based on the reader and card emulation mode is heterogeneous and the applications frequently interfere with the low RF parameters. Consequently, some applications cannot be pre-selected together because the RF parameters exposed to the reader may abort the transaction. The P2P technology offers an abstract interface to the RF technology and provides a bearer independent tunnelling between applications running in two devices. There are no longer conflicts related to the RF technology but only functional conflicts (e.g. possibly of payment from two means: ePurse or banking application). The application interface is identical irrespective of the P2P protocol stack (RF interface, P2P protocols, etc.) and irrespective of which device (the mobile terminal or the external device) has initiated the P2P communication. So the application issuer deploys one generic application.

4.15.2.10 Consideration about multiple HCI Hosts in card emulation mode

In a multi-HCI Host environment, it may happen that the HCI Hosts (and relevant applications) are not all supported by the same service provider. For example the terminal might support applications provided by a service provider while the UICC supports other applications provided by the mobile network operator or a third party supported by the mobile network operator.

In such an environment, each service provider should be responsible only for the services it supports.

At present, in case of a problem or question related to a mobile application (whether in the terminal or in the UICC), the end user will always apply to the MNO's customer care service.

In a multi-HCI Host environment, it is important that the end user can identify which application he is using, so that he can call the correct customer care and get the right answer without wasting time and money.

The new features brought by contactless services may cause more frequent calls to customer care. For example, conflicting or incompatible applications running in different HCI Hosts may bring new issues to the end user.

In order to minimize these issues, conflicts and incompatibilities management is delegated to one Managing Host in charge of solving these issues. This process may imply end-user interaction or may be automated in the Managing Host.

The Managing Host may be implemented in any of the HCI Hosts and need to have access to other HCI Hosts to get information from these HCI Hosts and their applications in order to be able to solve conflicts and generate a consolidated list of all the contactless applications available on the different active HCI Hosts.

The Managing Host is also responsible for implementing the selected model (i.e. aggregated versus non-aggregated):

- Aggregated model: A deployment model for multiple HCI Hosts on a single mobile device in which the end user selects from a collection of all services available in the mobile device and does not have to know where the associated contactless applications are hosted on the device.

- Non-aggregated model: A deployment model for multiple HCI Hosts on a single mobile device in which the end user selects a portfolio of services and all contactless applications in this portfolio are hosted in the same host.

The Managing Host also handles the configuration of the CLF (RF protocol parameters, routing table, etc.).

4.15.3 Requirements

4.15.3.1 Physical interface requirements

Identifier	Requirement
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 ETSI TS 102 221 [1] solution.
REQ-7-15-01-03	The solution shall be compatible with the existing form factors as defined in ETSI 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.
REQ-11-15-01-08	There shall be a means for the UICC to negotiate a higher supply current that will be made available while a contactless application is running.

4.15.3.2 Multi-protocol concurrent operation requirements

Identifier	Requirement
REQ-7-15-02-01	The UICC shall be capable of managing concurrently communication using both legacy protocol defined in ETSI 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	Requirement
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.

4.15.3.4 Compatibility with existing contactless systems requirements

Identifier	Requirement
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	Requirement
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	Requirement
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	Requirement
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.
REQ-12-15-07-03	There shall be an optional mechanism to inform the UICC about the current state of the User Interface of the device including the availability of the screen to display a message to the end user and the availability of the touchpad or keypad for the end user to input information.
REQ-12-15-07-04	The mechanism defined in REQ-12-15-07-03 shall be available for all UICC applications and not mandate the use of CAT (ETSI TS 102 223 [2]).
REQ-12-15-07-05	The following states shall be defined for the availability of the User Interface (UI) of the device: a) The UI is fully available, i.e. the screen is currently active and the Terminal application can display a message to the user and/or ask for a user input. b) The UI is locked and the user cannot be notified. c) The UI is locked and the user can be notified. d) The UI is unlocked but the user cannot be notified e) The UI state is unknown. See notes 1 and 2.
NOTE 1: The information provided by the Terminal is only accurate at the time it is delivered by the Terminal. NOTE 2: Notification of the user can also depend on the ability of the UICC application to communicate with the Terminal application and the ability of the Terminal application to activate the user interface.	

4.15.3.8 Interoperability requirements

Identifier	Requirement
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).
REQ-12-15-08-03	The CLFIP shall provide a means to detect and give an identity to any HCI Host connected to the CLF.
REQ-12-15-08-04	The CLFIP shall allow the transport of APDU between two HCI Hosts supporting the CLFIP.
REQ-12-15-08-05	The Managing Host shall be able to detect and solve conflicts between contactless applications hosted by different HCI Hosts.
REQ-12-15-08-06	The Managing Host shall implement both aggregated and non-aggregated models specified in GlobalPlatform's requirements for multiple secure elements [26].
REQ-12-15-08-07	The Managing Host shall be able to gather and consolidate information about the contactless applications provided by the different HCI Hosts, including application name and identifier, service provider name, logo, required RF parameters, customer support information and information about the preferred model (aggregated or non-aggregated) of the different HCI Hosts.
REQ-12-15-08-08	The Terminal Host, if present, shall be the Managing Host.
REQ-12-15-08-09	When NCI as specified in NCI v1.1 [27] or a later version is available, the Managing Host on the Terminal Host shall use NCI to handle configuration of the CLF (RF protocol parameters, routing table, etc.).
REQ-12-15-08-10	In case NCI v1.1 or a later version is not available, and if the CLF supports the configuration where the Managing Host's interface uses CLFIP, then the CLFIP shall provide means for the Managing Host to handle the configuration of the CLF (RF protocol parameters, routing table, etc.).
REQ-12-15-08-11	The Managing Host shall comply at least with the following rules: • The end user shall be able to choose the order of the list of contactless applications and the Managing Host shall not modify this order. • Each contactless application in the list shall be treated equally in term of space and information available on the user interface.
REQ-12-15-08-12	The CLFIP shall provide a means for a HCI Host to determine which is the Managing Host.

4.15.3.9 RFID requirements

Identifier	Requirement
REQ-10-15-09-01	The system made of the UICC and the terminal shall behave as a contactless reader based on the following standards: • ISO/IEC 18000 [20] Mode-3. • ISO/IEC 15693 [10].
REQ-10-15-09-02	The system made of the UICC and the terminal shall behave as a RFID tag based on the following standard: • ISO/IEC 15693 [10].
REQ-10-15-09-03	The interface between the UICC and the terminal shall be based on the CLFI (physical interface) and the CLFIP (communication protocol) as defined by ETSI TS 102 613 [18] and ETSI TS 102 622 [19].
REQ-10-15-09-04	The interface between the UICC and the terminal shall be independent of the RFID technology.
NOTE 1:	The ISO/IEC 15693 [10] standard is referenced in the ISO/IEC 18000 [20] standard series under ISO/IEC 18000-3 [20], Mode 1.
NOTE 2:	ISO/IEC includes this EPC air interface in the ISO/IEC 18000 [20] standard series under ISO/IEC 18000-3 [20], Mode- 3.

4.15.3.10 P2P mode requirements

4.15.3.10.1 General P2P requirements

Identifier	Requirement
REQ-11-15-10-1	Support of P2P mode shall be based on the HCI protocol as defined in ETSI TS 102 622 [19].
REQ-11-15-10-2	The CLFIP shall provide a means for the system consisting of the UICC and the terminal to support multiple active (i.e. exchanging data) applications in a host when operating in P2P mode.
REQ-11-15-10-3	The means provided by the CLFIP to support the P2P mode shall be identical irrespective of which device initiates the communication (e.g. terminal is generating the RF field or receiving the RF field).
REQ-11-15-10-4	The CLFIP shall provide a means allowing P2P mode to be used by the UICC in the "not battery powered" mode.
REQ-11-15-10-5	The CLFIP shall provide a means to notify all active hosts when all P2P channels are globally closed (e.g. loss of connection at the low level of the P2P protocol stack).
REQ-11-15-10-6	The CLFIP shall provide a means to convey application data having any size, even unknown, over the P2P protocol stack.
REQ-11-15-10-7	The means provided by the CLFIP to support the P2P mode shall be independent of the P2P protocol stack and its implementation.
REQ-11-15-10-8	The CLFIP shall provide a means to share the P2P data bandwidth between hosts.
REQ-11-15-10-9	The CLFIP shall provide means to inform the hosts about the data rate (excluding error recovery) of the actual connection between peer devices.
REQ-11-15-10-10	The CLFIP shall ensure that a P2P channel related to an application shall not block the data traffic of another P2P channel related to another application irrespective of the host.
REQ-11-15-10-11	The CLFIP shall support a P2P protocol stack ensuring reliable communications over a P2P channel toward another external device (e.g. ordered and error free).
REQ-11-15-10-12	The CLFIP shall provide a means allowing one P2P application in a host to initiate communication over one P2P channel while another application in the same host will wait for the peer device to initiate the communication.
REQ-11-15-10-13	The CLFIP shall provide a means allowing P2P applications to dynamically control the flow of data transmitted on each P2P channel for that application.
REQ-11-15-10-14	The CLFIP shall provide a means allowing an application to close one or all of its P2P channels.
REQ-11-15-10-15	The CLFIP shall provide a means to notify an application of its P2P channel state change (e.g. opened/closed).
REQ-11-15-10-16	The CLFIP shall provide a means for an application to exchange data over a P2P channel (e.g. send data/receive data).
REQ-11-15-10-17	The CLFIP shall provide a means allowing an application in a host to accept multiple P2P channels from the peer device.
REQ-11-15-10-18	The CLFIP shall provide a means allowing an application in a host to initiate one or more P2P channels to the peer device.

4.15.3.10.2 P2P application management requirements

Identifier	Requirement
REQ-11-15-10-19	P2P applications shall be uniquely identified by a service identifier.
REQ-11-15-10-20	The identity (service identifier) of a P2P application shall be unique independent of the P2P protocol stack implemented in the CLF.
REQ-11-15-10-21	The CLFIP shall provide a means allowing registration of the service identifiers and the pre-configuration of the P2P interface in order to allow an autonomous processing of the P2P protocol stack within the CLF.
REQ-11-15-10-22	The CLF shall allow the registration of a minimum of 16 service identifiers and a maximum of 255 per host.
REQ-11-15-10-23	The CLFIP shall provide a means so that each service identifier in the CLF is marked as being enabled or disabled: • when a service identifier is enabled then the CLF may establish a P2P channel using this service identifier; • when a service identifier is disabled the CLF cannot establish a P2P channel using this service identifier.
REQ-11-15-10-24	The CLFIP shall provide a means so that a host can disable all at once all of its service identifiers registered in the CLF.
REQ-11-15-10-25	The CLFIP shall provide a means so that a host can disable any of its service identifiers registered in the CLF.
REQ-11-15-10-26	The CLFIP shall provide a means so that when a host has disabled one or several of its services identifiers registered in the CLF only this host can re-enable this/these service identifier(s).
REQ-11-15-10-27	The CLFIP shall provide a means to inform all hosts when a host registers a P2P application.
REQ-11-15-10-28	The CLFIP shall provide a means for a host to gather information about a P2P application in another host which can be used to resolve any conflicts or incompatibilities (possibly with user input).
REQ-11-15-10-29	This information shall contain at least the service identifier and the reference of the relevant host as registered in the CLF.
REQ-11-15-10-30	The CLFIP shall provide a means for a host to gather information about another host which can be used to resolve any conflicts or incompatibilities (possibly with user input).
REQ-11-15-10-31	This information shall contain: • the name of the issuer of the host; • a short description of the host; • the customer care access information (e.g. phone number, URI, email address).
REQ-11-15-10-32	It shall be possible that this information also contains an information logo.
REQ-11-15-10-33	The CLFIP shall provide a means for the managing host' to be identified.
REQ-11-15-10-34	The managing host shall be responsible for detecting and resolving conflicts or incompatibilities between applications and between hosts.
REQ-11-15-10-35	The CLFIP shall provide a means to allow the managing host to notify the CLF that the managing host has detected a conflict or an incompatibility concerning a host.
REQ-11-15-10-36	The CLFIP shall provide a means so that the CLF receiving from the managing host such a notification about a host shall disable (no P2P channel can be established) all at once (one command, no need to provide a list) all of the service identifiers of this host registered in the CLF.
REQ-11-15-10-37	The CLFIP shall provide a means to allow the managing host to notify the CLF that the managing host has detected a conflict or an incompatibility concerning an application registered in the CLF.
REQ-11-15-10-38	The CLFIP shall provide a means so that the CLF receiving from the managing host such a notification shall disable (no P2P channel can be established) the service identifier of this application registered in the CLF.
REQ-11-15-10-39	The CLFIP shall provide a means to allow the managing host to notify the CLF that a service identifier disabled due to conflict or incompatibility can be re-enabled.
REQ-11-15-10-40	The CLFIP shall provide a means so that the CLF upon a notification as per REQ-10-15-10-35 shall re-enable the service identifier concerned (provided the service identifier has not been disabled by its proper host).
REQ-11-15-10-41	It shall be possible to configure the CLF so that the UICC is the default managing host.
REQ-11-15-10-42	The CLFIP shall provide a means for the user to select or change the managing host through a user interface on the terminal.
REQ-11-15-10-43	The CLFIP shall provide a means to notify all hosts about the new managing host when the managing host is changed.
REQ-11-15-10-44	The CLFIP shall provide a means to get the status of all the P2P services in the CLF (e.g. enabled/disabled).

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 will 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, etc.) 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, etc.);

    - 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 will 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, etc.);

- 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^{TM}, NFC, ZigBee^{TM}, etc.);

- via a Wi-Fi network inside a Bank area (potentially protected environment);

- via a Wi-Fi network outside a Bank area (potentially unprotected environment);

- etc.

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, etc.);

- possibly define proprietary algorithms and protocols to manage the end-to-end connection;

- possibly interact with external peripherals (Bluetooth^{TM}, etc.);

- 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, etc.);

- the possibility to interact with external peripherals such as Bluetooth^{TM} (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;

- the possibility to use existing personalization systems or schemes that require a chaining of commands within a sequence to facilitate these activities.

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, etc.);

  - 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, etc.);

- 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;

- the possibility to use existing personalization systems or schemes that require a chaining of commands within a sequence to facilitate these activities.

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 customization 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;

- 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, etc.);

- 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;

- 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

4.17.3.0   General

This clause defines the requirements for confidential applications.

4.17.3.1   Confidential application environment

Identifier	Requirement
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.
REQ-9-17-01-09	Security mechanisms for the administration of third party areas shall include state-of-the-art developments in cryptography.

4.17.3.2 Administration by Card issuer

4.17.3.2.1 Third party area environment administration

Identifier	Requirement
REQ-8-17-02-01	A card issuer shall be able to manage third party areas by the following means: • At personalization. • 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	Requirement
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	Requirement
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-9-17-04-05	For applications based on the CAT Runtime Environment as defined in ETSI TS 102 241 [16], 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, etc.).
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.
REQ-9-17-04-10	For applications based on an "Enhanced Runtime Environment". the third party policy shall include its allowed access and restriction to APIs at a package and method level.

4.17.3.3 Administration by Third party

Identifier	Requirement
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, etc.).
REQ-9-17-05-09	A mechanism shall be defined that allows the chaining of commands for the personalization of applications.
REQ-9-17-05-10	A mechanism shall be defined that allows the use of "online mode" for the personalization of applications, i.e. sending the next command only after receiving the response to the previous one.

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	Requirement
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 ETSI TS 102 221 [1].

- Card Application Toolkit ETSI 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 categorized 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, car equipment 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

4.18.2.1.0   General

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/IEC 16750-3 [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] requirements and be delivered with PPAP (production part approval process) documentation;

- with class E as defined in ISO/IEC 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 minimize 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 optimize 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 minimize 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 is 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 minimize 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

4.18.2.2.0 General

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 minimized, which requires also the size of the M2M UICC to be minimized. Metering devices may be produced in high volumes, which requires that the M2M UICC can be integrated in an industrialized 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 minimize 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 minimized, which requires also the size of the MFF to be minimized. 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 minimize 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 minimized, which requires also the size of the MFF to be minimized. In many cases the device will 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 minimize 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 minimize 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 optimization 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 minimize 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 optimization 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

4.18.3.0 General

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

4.18.3.1.0 General

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.
REQ-12-18-01-04	There shall be a mechanism for an M2M UICC to store information about the supported environmental conditions and classes as defined in ETSI TS 102 671 [25].
REQ-12-18-01-05	It shall be possible to retrieve the information about supported environmental conditions and classes as defined in ETSI TS 102 671 [25] from the M2M UICC.

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 ETSI 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 ETSI 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 characterized 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 realized 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 minimized.
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 personalization.
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 will 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

Identifier	Requirement
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 ETSI EN 300 468 [11] and ETSI 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)

ETSI 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 minimizes 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)

4.21.2.0 General

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, etc.), 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.

4.22 Multicast dataflow in UICC

4.22.1 Abstract (informative)

The Release 8 UICC capabilities, combined with existing broadcasting network system may allow to deploy new services such as data broadcast or Mobile-TV related services. This clause lists the corresponding use cases and requirements.

4.22.2 Use cases (informative)

4.22.2.1 Use case - Broadcast data services

Several broadcasting network transmissions are currently deployed, for example MBMS, DVB-H and FLO. They are currently used for but not limited to video. All are based on multicast functionality, which allows an application to subscribe to a specific service on a host, and when this host is receiving data broadcast related to the identified service, the host will forward the message only to the registered application. This feature allows to rationalize data distribution and increase bandwidth efficiency in transmission networks.

With IP capabilities combined with multicast functionalities, this new communication channel would allow to provision a large range of UICC with a single message, for example provisioning data or files for a specific application, or distributing multimedia content teasing.

4.22.2.2 Use case - Mobile TV related services

For specific Mobile-TV related services, the UICC could receive directly data broadcast. The UICC would provide services associated with this flow, such as:

- service presentation functionalities (i.e. personalization of the electronic service guide in the UICC managed according to data related to the user profile residing in the UICC); or

- update of application related to Mobile-TV security management (such as CAS application).

4.22.3 Requirement for multicast dataflow (subscription and dataflow reception)

Identifier	Requirement
REQ-9-22-01-01	There shall be a mechanism allowing the UICC to discover, subscribe and unsubscribe to multicast dataflow.
REQ-9-22-01-02	There shall be a mechanism allowing the UICC to receive and suspend the corresponding multicast dataflow.
REQ-9-22-01-03	This multicast dataflow subscription mechanism and reception mechanism shall be compatible with IP.
REQ-9-22-01-04	There shall be means to authenticate and/or decipher the incoming dataflow in the UICC.
REQ-9-22-01-05	The multicast dataflow mechanisms (subscription and dataflow reception) shall be available only for authorized applications (e.g. application allowed to use USB, IP resources).
REQ-9-22-01-06	A mechanism for managing the authorized application list in the UICC shall be described.
REQ-9-22-01-07	The multicast dataflow mechanisms shall be optional for the UICC and the Terminal.

4.22.4 Interaction with existing features (informative)

None.

4.23 New type of data storage and access

4.23.1 Abstract (informative)

The memory technology and the capability for the UICC to host large amounts of data as well as new types of data mean that there is a need to improve data storage and management in the UICC.

This clause lists use cases and associated requirements for a new type of data storage and access.

4.23.2 Background (informative)

4.23.2.0 General

This clause lists the use cases relevant for new types of data storage and access.

4.23.2.1 Use case - Taking a picture from the terminal, storing it on the UICC and retrieving it

The UICC is a secure element where a multimedia application residing on the terminal could store the data managed by this application. For example, a camera could store pictures directly on the UICC and an application dedicated to explore multimedia content could access this content, like any secure element or storage medium associated with the terminal.

In such a use case a mechanism has to be defined in order to control the usage of the UICC by the camera application on the terminal which may lead to memory consumption beyond the control of the card issuer. A secure mechanism has to be defined in order to manage memory allocation parameters.

In addition, a secure mechanism is required to prevent unauthorized access to the pictures stored in the UICC.

For this use case, the user should be able to rename picture files, delete picture files, create directories and move files between directories. Picture files and directories should support meaningful names.

The device using the UICC may support different types of picture files and movies, so a mechanism to identify file types is needed.

The clause dedicated to New UICC-Terminal Interface of the present document already described several use cases related to multimedia data management.

4.23.2.2 Use case - Storing and protecting data through operator portal

The end-user browsing the MNO portal can access content either stored in the UICC during the personalization of the UICC or retrieved from the MNO server and stored by the end-user on the UICC. This content could be an interactive subscription guide or HTML pages describing card issuer services. Such data could be MNO specific (such as an HTML service description or logo) and might need some specific features such as being invisible for the end-user and with no deletion right.

4.23.2.3 Use case - Storing a service description

The UICC stores some information in a specific format, such as in XML files, describing a service. This formatted information could be retrieved and interpreted by an appropriate application.

4.23.2.4 Use case - Managing multimedia content via UICC to a remote server

If the service is available or if the end-user subscribed to such a service, the end-user is able to request that the UICC saves personal content (such as picture, videos, etc.) to a remote server.

4.23.2.5 Use case - Partitioning UICC memory

In order to monetize large memory UICC, the card issuer could offer the capability to divide the memory of such a UICC into partitions for different players such as user or content provider. For example, a part of the UICC memory could be allocated to the end-user content, allowing him to download multimedia or applications in this memory area. The UICC in that case would have to provide a security mechanism to make sure the memory is controlled by the end-user or card issuer.

4.23.2.6 Use case - UICC content depending on user authentication

In order to protect end-user content, when being stored in the UICC, one can imagine that different types of content will be visible in the UICC to the end-user. The visibility of this content would be determined by the levels of security defined for the content.

4.23.2.7 Use case - Migration to a USB UICC without ICCD class

It is possible to optimize a USB UICC implementation so that the ICCD class is not required. In order to ease migration of existing services to a UICC supporting USB interface without support of the ICCD class, support of existing file types (e.g. cyclic, transparent, linear fixed, BER-TLV) would be provided.

4.23.3 Requirements

4.23.3.1 Data storage and structure requirements

Identifier	Requirement
REQ-9-23-01-01	There shall be a mechanism to store to and retrieve data from a file in the UICC (e.g. picture, video, ringtone, wall paper, screen saver, notes, text file, application code, etc.).
REQ-9-23-01-02	Each file shall be addressable via a name.
REQ-9-23-01-03	It shall be possible to associate the type of data together with the data.
REQ-9-23-01-04	It shall be possible to group the files in a directory hierarchy.
REQ-9-23-01-05	It shall be possible to list the content of a directory including the type of data of each file.
REQ-9-23-01-06	It shall be possible to separate the UICC memory into partitions.

Identifier	Requirement
REQ-9-23-01-07	It shall be possible to perform at least the following actions: • Read, write, create, resize and delete file. • Read or write random access to file. • Create linked file and directory. • Create and delete directory. • Move or copy a file within a hierarchy without changing the access rights on the file. • Create, delete and resize a partition.
REQ-9-23-01-08	The consequences of deleting a file, directory or a partition shall be clearly specified.
REQ-9-23-01-09	In case of file, directory or partition deletion, the released memory shall be recovered.
REQ-9-23-01-10	A mechanism shall be provided to manage error cases when file administration cannot be performed due to UICC or partition memory overflow.
REQ-9-23-01-11	A mapping of ETSI TS 102 221 [1] file types, their behaviour and limits (e.g. cyclic, transparent, linear fixed, BER-TLV) to new file types shall be provided.

4.23.3.2 Data protection requirements

Identifier	Requirement
REQ-9-23-02-01	There shall be a mechanism to secure specific files, directories and partitions.
REQ-9-23-02-02	This mechanism shall allow several levels of security depending on entity accessing the data and the type of content accessed.
REQ-9-23-02-03	There shall be a mechanism to set and change the file, partition and directory access right.
REQ-9-23-02-04	The security mechanism shall implement the security policy for the following entities to access the data: • An application residing in the UICC, owned either by a third party or the card issuer. • An application residing in the terminal or another device hosting the UICC.
REQ-9-23-02-05	The security mechanism shall manage different access rights depending on the application owner.
REQ-9-23-02-06	The security mechanism shall allow the following types of content to be accessed: • Card issuer-generated or modified content. • Third party-generated or modified content. • End-user-generated or modified content.
REQ-9-23-02-07	There shall be a mechanism to limit the UICC memory allocated for applications.
REQ-9-23-02-08	There shall be a security mechanism specified to authenticate an application before allowing it to store or access data in the UICC.
REQ-9-23-02-09	The security mechanism shall differentiate between the actions listed in REQ-9-23-01-07.
REQ-9-23-02-10	A mechanism shall be provided that assures the integrity of file, directory and partition in case of power interruption (e.g. unexpected power loss or unexpected remove of the UICC from the device).
REQ-9-23-02-11	It shall be possible to apply this mechanism on selected files.

4.23.3.3 Local and remote access requirements

Identifier	Requirement
REQ-9-23-03-01	There shall be a set of commands specified that allow for the actions listed in REQ-9-23-01-07 after an appropriate security check.
REQ-9-23-03-02	There shall be a mechanism specified allowing to perform remotely all actions as listed in REQ-9-23-01-07 after appropriate security check.
REQ-9-23-03-03	There shall be a mechanism specified to provide consistency in case of simultaneous access to data (e.g. local access and remote access, or application access and local access).

4.23.4 Interaction with existing features (informative)

Interaction with Confidential Applications is expected as there is a requirement that limits the memory used by applications residing in the UICC.

4.24 CAT access over a modem interface

4.24.1 Abstract (informative)

Mobile modems are becoming a significant sector of the mobile communications market. The architecture is based on three entities: the modem, the UICC and the entity connected to the modem. This connected entity may be a PC or a Machine to Machine device. Currently support for CAT in these entities is being limited by the lack of standards defining how CAT should be extended to applications running in the connected entity through the interface between the modem and the connected entity. It will be noted that in the view of CAT, applications in the connected device offer CAT services to UICC applications. This clause details use cases and requirements for a new feature that extends the CAT functionality to entities connected to a modem, over the modem - client interface.
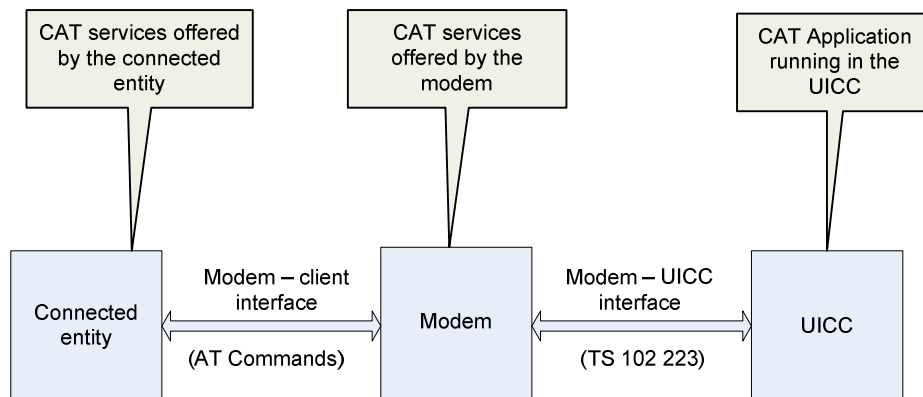
Figure 5: CAT Services and Applications

4.24.2 Background (informative)

4.24.2.0 General

This clause details the use cases that justify the requirements for the extension of CAT commands over the modem - client interface.

4.24.2.1 Use case - Extending CAT to the connected entity capabilities

Currently, modems are unable to fully take advantage of services offered by CAT. These services may be essential to the ease of use of the network services, such as validated airtime credit. In other cases these CAT applications may deliver additional value added services for the customer. It is typical for mobile modems to be sold with PC applications that make it easy for the user to connect to a data network. These PC applications may provide functionality that makes use of some basic CAT support, such as DISPLAY TEXT, PLAY TONE or GET INPUT.

It is important that existing CAT applications on existing UICCs work seamlessly with the CAT access over a modem interface feature defined in this clause and desirable that a new UICC that supports the CAT access over a modem interface feature can direct CAT commands to either the modem or the PC client explicitly.

In this use case the CAT functionality is extended over the modem-client interface to one or more application in the PC which then performs the CAT commands in a similar way to current terminals that support CAT. In this use case, the modem-client interface is typically an AT command interface as detailed in ETSI TS 127 007 [17].

As UICC applications are often security-related, it may be necessary for UICC CAT applications to be able to authenticate the connected entity and to be able to securely exchange data between the UICC CAT applications and the connected entity.

As the PC application's support of CAT may be different to the modem support of CAT, it is expected that the modem will inform the UICC that it supports the combined functionality of the modem and the PC application. Some CAT commands are only relevant for the modem and it is expected that these will not be passed to the PC application. Additionally a PC application may be started and shut down independently of the UICC session, so a mechanism is needed that allows a PC application to add and remove its CAT functionality.

A PC may host additional applications making use of CAT in addition to any applications delivered with the modem, which provide some basic services. Examples might be one application providing CAT access to a second card reader and another application that connects to an external GPS device via Bluetooth^{TM} to receive positional data.

4.24.2.2   Use case - Using CAT for data acquisition and control in an M2M device

This feature introduces the possibility for applications on the UICC to interact with applications deployed on a machine to machine device (M2M device applications). The modem-client interface is typically an AT command interface as detailed in ETSI TS 127 007 [17].

In this scenario, CAT is used to provide secure network data transfer to/from the M2M device applications and to control the M2M device. The Modem access to CAT feature extends the AT command set, enriching the M2M services with the security and manageability strengths of the UICC.

In this use case, it is envisioned that UICC applications are able to identify the M2M device applications and that encryption/decryption of the communication is performed outside of the present document.

As the M2M device application's support of CAT may be different to the modem support of CAT, it is expected that the modem will inform the UICC that it supports the combined functionality of the modem and the M2M device application. Some CAT commands are only relevant for the modem and it is expected that these will not be passed to the M2M device application. Additionally the M2M device application may be started and shut down independently of the UICC session, so a mechanism is needed that allows the M2M device application to add and remove its CAT functionality.

4.24.2.3   Use case - Addition of CAT support by adding a CAT extender device

Modems may optionally support letter class features of CAT and typically have reduced capability, as described in the present document. This feature introduces the possibility to extend the modem support for CAT by the addition of a CAT extender device that offers additional functionality (such as a card reader or a display).

As the CAT extender device support of CAT will be different to the modem support of CAT, it is expected that the modem will inform the UICC that it supports the combined functionality of the modem and the CAT extender device. Some CAT commands are only relevant for the modem and it is expected that these will not be passed to the CAT extender device. Additionally the CAT extender device may be started and shut down independently of the UICC session, so a mechanism is needed that allows the CAT extender device to add and remove its CAT functionality.

4.24.3   Requirements

4.24.3.1   General requirements

Identifier	Requirement
REQ-9-24-01-01	Support for the CAT functionality over the modem interface using AT commands shall be optional for the connected entity, the modem and the UICC.
REQ-9-24-01-02	A modem supporting the CAT functionality over the modem interface shall also support both CAT as defined in ETSI TS 102 223 [2] and the AT interface as defined in ETSI TS 127 007 [17].
REQ-9-24-01-03	All CAT communication with the UICC via the modem shall use the CAT protocol defined in ETSI TS 102 223 [2].
REQ-9-24-01-04	All CAT communication with the connected entity via the modem shall use the AT interface as defined in ETSI TS 127 007 [17], extended by the requirements detailed in this section for new AT commands.
REQ-10-24-01-05	The modem shall allow multiple connected entities to be registered for the CAT functionality over the modem interface feature.
REQ-9-24-01-06	CAT applications on UICCs that are not aware of the CAT functionality over the modem interface shall be able to use the legacy support of this feature.
REQ-9-24-01-07	CAT applications on UICCs that are aware of the CAT functionality over the modem interface shall be able to use the legacy support and the extended support of this feature if the modem supports it.
REQ-11-24-01-08	Modem and/or connected entities support for this feature shall be indicated in the CAT TERMINAL PROFILE.

4.24.3.2 Connected device registration requirements

Identifier	Requirement
REQ-9-24-02-01	AT command(s) shall be specified that allow a connected entity to register for CAT commands over the modem interface.
REQ-11-24-02-02	The registration request shall allow the identification of the connected entity using a text string (extended mode only).
REQ-9-24-02-03	The registration request shall allow the connected entity to detail the CAT features that it supports by sending data similar to the TERMINAL PROFILE detailed in ETSI TS 102 223 [2].
REQ-9-24-02-04	In reply to the registration request from the connected entity, the modem shall confirm to the connected device that it both supports the CAT functionality over the modem interface feature and that it successfully updated the terminal profile with the UICC, by the OK response.
REQ-9-24-02-05	If the registration request is not understood or if the modem cannot successfully update the terminal profile with the UICC, the modem shall return an error response.
REQ-9-24-02-06	Once a connected entity has registered, the modem shall send any relevant CAT commands to the connected entity and accept any supported events and command responses from the connected entity.

4.24.3.3 Legacy support requirements

Identifier	Requirement
REQ-9-24-03-01	On receipt of a valid registration request from the connected device, the modem shall generate a combined terminal profile from the information supplied and the modems own terminal profile, as detailed in table 1.
REQ-9-24-03-02	The modem shall send the combined Terminal profile to the UICC using the TERMINAL PROFILE command.
REQ-9-24-03-03	If the UICC does not explicitly indicate whether a CAT command shall be sent to the modem or the connected entity, the CAT commands received by the modem from the UICC shall be processed using the rules described in table 2.
REQ-10-24-03-04	When a connected entity requests registration, it shall be informed of which commands are available to be executed by the connected entity in legacy mode.
REQ-10-24-03-05	In legacy mode, the modem shall allocate the routing of each command to the requesting connected entity if that command is not already registered to the modem or another connected entity at the time of the registration request.

Table 1: Rules for combining the Terminal Profile

Feature	Rule for combined Terminal profile
Call control by NAA	Set only if supported by the modem
MO short message control support	Set only if supported by the modem
PROVIDE LOCAL INFORMATION (MCC, MNC, LAC, Cell ID & IMEI)	Set only if supported by the modem
PROVIDE LOCAL INFORMATION (NMR)	Set only if supported by the modem
POLL INTERVAL	Set only if supported by the modem
POLLING OFF	Set only if supported by the modem
Event: MT call	Set only if supported by the modem
Event: Call connected	Set only if supported by the modem
Event: Call disconnected	Set only if supported by the modem
Event: Location status	Set only if supported by the modem
Event: Access Technology Change	Set only if supported by the modem
Event: Network Search Mode Change	Set only if supported by the modem
Fourteenth byte (Screen height), Fifteenth byte (Screen width) and Sixteenth byte (Screen effects)	If the connected entity does not have ND set then: • the Fourteenth, fifteenth and sixteenth byte shall be as for the connected entity else • the Fourteenth, fifteenth and sixteenth byte shall be as for the modem
PROVIDE LOCAL INFORMATION (ESN)	Set only if supported by the modem
Call control on GPRS	Set only if supported by the modem
PROVIDE LOCAL INFORMATION (IMEISV)	Set only if supported by the modem
PROVIDE LOCAL INFORMATION (Search Mode change)	Set only if supported by the modem
PROVIDE LOCAL INFORMATION (NMR(UTRAN))	Set only if supported by the modem
Steering of Roaming for I-WLAN REFRESH support	Set only if supported by the modem
All other features	Set if supported by either the modem or the connected entity

Table 2: Rules for deciding where CAT commands are executed

Feature	Command executed by
PROVIDE LOCAL INFORMATION (MCC, MNC, LAC, Cell ID & IMEI)	Only by the modem
PROVIDE LOCAL INFORMATION (NMR)	Only by the modem
PROVIDE LOCAL INFORMATION (ESN)	Only by the modem
Call control on GPRS	Only by the modem
PROVIDE LOCAL INFORMATION (IMEISV)	Only by the modem
PROVIDE LOCAL INFORMATION (Search Mode change)	Only by the modem
PROVIDE LOCAL INFORMATION (NMR(UTRAN))	Only by the modem
Steering of Roaming for I-WLAN REFRESH support	Only by the modem
POLL INTERVAL	Only by the modem
POLLING OFF	Only by the modem
All other commands	According to requirement REQ-10-24-03-05, if any of the connected entity supports the command Otherwise it shall be executed by the modem

4.24.3.4 Extended support requirements

Identifier	Requirement
REQ-9-24-04-01	The CAT defined in ETSI TS 102 223 [2] shall be extended to allow applications in UICCs that support the CAT functionality over the modem interface feature to discover the individual terminal profiles.
REQ-11-24-04-02	The CAT defined in ETSI TS 102 223 [2] shall be extended to allow applications in UICCs that support the CAT functionality over the modem interface feature to select whether each CAT command shall be sent in the same way as for legacy mode or in extended mode indicating explicitly the target entity.
REQ-11-24-04-03	The CAT defined in ETSI TS 102 223 [2] shall be extended to allow applications in UICCs that support the extended CAT functionality over the modem interface feature to be notified when connected entities initiate their session in extended mode.

4.24.3.5 CAT over modem-client interface requirements

Identifier	Requirement
REQ-9-24-05-01	CAT commands shall be sent to the connected entity using an unsolicited result code defined for this purpose on the AT command interface.
REQ-9-24-05-02	The connected entity shall execute the command in accordance with ETSI TS 102 223 [2] and create a response.
REQ-9-24-05-03	The response shall be sent from the connected entity to the modem using a specific AT command designed for this purpose.
REQ-9-24-05-04	If the connected device interface is terminated before the response to the CAT command is received then the modem shall send a Terminal Response to the UICC with the response code set to - 'Terminal currently unable to process command'.
REQ-9-24-05-05	CAT events shall be able to be sent by the connected entity using a specific AT command designed for this purpose.
REQ-9-24-05-06	The modem shall forward events to the UICC with the exception of the following events: • Event: MT call. • Event: Call connected. • Event: Call disconnected. • Event: Location status. • Event: Access Technology Change. • Event: Network Search Mode Change.
REQ-9-24-05-07	The modem shall be able to indicate at least the following in response to a CAT event AT command: • event successfully delivered to the UICC; • event failed to be sent the UICC as the modem is busy; • event not allowed from connected entity; • event rejected by the UICC.

4.24.3.6 Connected entity termination requirements

Identifier	Requirement
REQ-9-24-06-01	AT commands(s) shall be specified that allow a connected entity to terminate the current CAT commands over the modem interface session.
REQ-9-24-06-02	On receipt of the session termination request, the modem shall send its TERMINAL PROFILE to the UICC.
REQ-9-24-06-03	On receipt of the session termination request, the modem shall stop sending CAT commands to the connected entity.
REQ-9-24-06-04	Following the session termination request, the modem shall reject all CAT events from the connected entity.
REQ-11-24-06-05	An additional proactive command shall be defined to request the modem to terminate current extended mode session with the connected entity and the modem shall inform the connected entity that the session has been terminated.

4.24.3.7 Security requirements

Identifier	Requirement
REQ-10-24-07-01	It shall be possible for the UICC CAT applications to authenticate the connected entities.
REQ-10-24-07-02	It shall be possible for a UICC CAT application and a connected entity to encrypt/decrypt the data that is exchanged between them.
REQ-10-24-07-03	It shall be possible for a UICC CAT application and a connected entity to check the integrity of the data that is exchanged between them.

4.24.4 Interaction with existing features (informative)

This feature interacts with CAT, secure channels, reduced capability terminal and the applicative protocol feature.

There are also secure channel requirements to protect toolkit related traffic. To reduce the proliferation of mechanisms to secure channel related functionality, the mechanisms could be aligned.

4.25 UICC-Terminal applications and services over USB

4.25.1 Abstract (informative)

Release 7 introduces TCP/IP protocol stack for the UICC in ETSI TS 102 483 [21], allowing the UICC to become a part of the IP network. In Release 8, only frameworks available for the applications running in the UICC, that are designed to use the APDU protocol (over ISO or USB ICCD interface), were defined. To migrate the UICC to full IP, there is a need to design a new framework for applications and services development (i.e. applications running in the UICC and/or in the terminal), providing all the benefits of USB and the IP layers.

With an IP stack implemented in the UICC, applications will be able to use any type of protocol based on TCP or UDP, such as FTP, HTTP, SIP and RTP. When the APDU protocol is not used, this new framework will use the USB EEM interface and allow Internet Protocol based applications to send commands to as well as receive events from the terminal, and vice versa.

This new framework is composed of services. Applications can make use of these services which run either in the terminal or in the UICC. The new framework defines how the services provided by the framework are discovered and invoked by applications (i.e. service discovery and service invocation). As an example, UICC applications may use services running either in the terminal or in the UICC. Moreover, terminal applications may use services in the same way. Thanks to the framework, the service location may be transparent to the applications.

This new framework may be used by any application relying on the UICC platform. For example, applications defined by 3GPP (USIM, ISIM, etc.) may take benefit of this new framework.

This clause defines use cases and requirements for such a framework and for the services that it will support.

4.25.2 Background (informative)

4.25.2.1 Use case - Migration of existing services over IP

For Release 9 UICC and terminals, when the USB interface is activated and the IP layer is available, execution of actions such as sending SMS or setting up a call are not defined for the IP layer. The proactive services provided by ETSI TS 102 223 [2] are only inherited on the USB ICCD interface carrying APDUs on USB. The migration of such services to the new framework provides the following benefits:

- A consistent and efficient usage of all interfaces available on the UICC.

- A mechanism to send immediately proactive commands as defined in ETSI TS 102 223 [2] even if there is no activity over the USB ICCD interface.

4.25.2.2   Use case - End-user interaction

UICC based applications should be able to use modern user interface technologies, which can be provided by new services over the USB interface. These services can be adapted to end-user usage and habits.

- Scenario 1: A user dialog proposes the storage of a document securely inside a memory card in the terminal using this framework to access that data allowing the UICC to encrypt/decrypt the data.

- Scenario 2: Using this framework, the user is able to enter, access and synchronize his contact information in the contact manager application in the UICC and applications residing in the terminal, in a connected device or in a remote server.

- Scenario 3: Using this framework, the user can access services provided by the UICC from his PC through, for example, Bluetooth^{TM} or a USB cable.

- Scenario 4: Using this framework, the user is presented with content such as applications, pictures, video or audio, residing on the UICC making use of the broad capabilities of terminal media management.

- Scenario 5: Using this framework, the user will be able to interact with applications residing in the UICC via new technologies integrated in the terminal (e.g. motion sensors or a touch screen).

- Scenario 6: When accessing some sensitive valuable services (e.g. accessing web pages to be billed on a data subscription or using banking related application), the end-user might have to enter sensitive information such as PIN code or password. Using this framework, the interface could be secured and the user could be provided with an indication that the interface is actually secured.

4.25.2.3   Use case - Integration of UICC services into terminal user interface

Selected content in the UICC can be seamlessly integrated in the terminal's user interface providing the terminal with the content/application type information.

- Scenario 1: Using this framework and the type information provided by it, the terminal can present play lists based on valid access rights of certain content of the UICC (e.g. in the multimedia player application).

- Scenario 2: Using this framework, the terminal can use the provided type information to organize access to the applications in the UICC, for example a games application would appear in the "Game" menu using its own icon.

- Scenario 3: When the user browses on his favourite internet website, his Email account for instance, he may configure the browser in order to store securely the sites login and password in the UICC.

4.25.2.4   Use case - Access status of communication services

In addition to existing legacy services, some applications running on the UICC need to have access to the status of the data channel (channel available or not, type of data channel) in order to be able to adapt their behaviour or to propose specific services, for example temporary storage of data when no connection available and later synchronization.

4.25.2.5   Use case - Access to specific terminal hardware

Enabling the UICC to access peripherals allows the following scenarios:

- Scenario 1: Accessing the Camera can give the UICC the opportunity of directly accessing data vision and allowing security services based on data vision (e.g. a bar code).

- Scenario 2: Biometric sensors can authorize user operation replacing the existing knowledge-based user authentication mechanism (i.e. PIN verification).

- Scenario 3: If the UICC is able to access and control the peripherals, it would be possible to for example request access to the Global Positioning System (GPS), get the current coordinates, release the GPS system resource and then send the coordinates to the network as input for tracking applications.

Typical peripherals include: camera, biometric sensors, GPS interface, local connectivity interfaces (Bluetooth™, USB terminal interface, Infrared, LAN network interfaces, etc.), accelerometer, touch screen, keyboard, audio synthesizer and vibrating system, and additional memory devices.

4.25.2.6 Use case - Interaction between terminal and UICC applications

UICC and terminal applications are able to discover and interact with available applications and services on both sides such as contact manager, multimedia player, Web browser and Wi-Fi authentication services.

- Scenario 1: When a user launches an application stored in the UICC, this application has the possibility to:

  - Call and launch the terminal's applications to support it.

  - Use the terminal's services associated with this application.

  - Close terminal's applications launched by the UICC itself.

- Scenario 2: The UICC and terminal provide services to authorized applications of the other entity. For example, the UICC offers a service of network authentication to a Wi-Fi network.

4.25.3 Requirements

4.25.3.1 General framework requirements

Identifier	Requirement
REQ-10-25-01-01	The framework shall only use the USB UICC interface with USB EEM class and TCP/IP (as defined in ETSI TS 102 483 [21]) for communication with the terminal.
REQ-10-25-01-02	The framework shall provide a set of services available to the UICC and/or the terminal (framework services).
REQ-10-25-01-03	The framework shall provide a set of procedures in order to setup and manage the framework itself such as capabilities exchange, discovery mechanism and dynamic update.
REQ-10-25-01-04	The framework shall provide a set of commands exchanged over the UICC-Terminal interface corresponding to service invocation and execution.
REQ-10-25-01-05	The framework shall provide means to allow interaction between applications residing in the UICC and applications residing in the terminal.
REQ-10-25-01-06	Services provided by the framework shall be available to the terminal and UICC as well as to any device connected to the terminal.
REQ-10-25-01-07	The framework shall be designed such as it can be extended and new services can be added.

4.25.3.2 Framework service discovery and management requirements

Identifier	Requirement
REQ-10-25-02-01	The framework shall provide means for allowing the UICC and terminal to publish their services.
REQ-10-25-02-02	The framework shall provide means for allowing the UICC and terminal to discover their respective services.
REQ-10-25-02-03	Each framework service shall be uniquely identified.
REQ-10-25-02-04	The framework shall provide means for the applications to control and invoke a service.
REQ-10-25-02-05	The framework shall provide means to dynamically notify the UICC and terminal of service updates.

4.25.3.3 Interaction between UICC and terminal applications requirements

Identifier	Requirement
REQ-10-25-03-01	A framework service shall be defined allowing the UICC and terminal to publish their applications.
REQ-10-25-03-02	A framework service shall be defined allowing the UICC and terminal to discover their respective applications.
REQ-10-25-03-03	In the context of the framework each terminal application shall be uniquely identified.
REQ-10-25-03-04	In the context of the framework each UICC application shall be uniquely identified.
REQ-10-25-03-05	A framework service shall be defined allowing UICC applications to launch terminal applications.
REQ-10-25-03-06	A framework service shall be defined allowing UICC applications to close terminal applications that have been launched by the UICC.
REQ-10-25-03-07	A framework service shall be defined allowing terminal applications to launch UICC applications.
REQ-10-25-03-08	A framework service shall be defined allowing terminal applications to close UICC applications that have been launched by the terminal.
REQ-10-25-03-09	The framework shall provide means to dynamically notify the UICC and terminal of application updates.

4.25.3.4 Framework security requirements

Identifier	Requirement
REQ-10-25-04-01	The framework shall provide means to manage security policies regarding the access to the services and applications provided by the terminal and the UICC.
REQ-10-25-04-02	The framework shall provide means to secure communications between an application and a service (e.g. confidentiality, authentication and integrity).
REQ-10-25-04-03	The framework shall provide means to secure (e.g. confidentiality, authentication and integrity) communications between an application residing in the UICC and an application residing in the terminal or in a connected device.

4.25.3.5 User Interface requirements

Identifier	Requirement
REQ-10-25-05-01	Framework services shall be defined allowing the UICC to deliver media content to the terminal (e.g. web content, text, audio, pictures, video and JavaScript).
REQ-10-25-05-02	A framework service shall be defined allowing the UICC to use all the terminal MMI output capabilities.
REQ-10-25-05-03	A framework service shall be defined allowing the UICC to use all terminal MMI input capabilities (e.g. Keyboard, touch screen, microphone, camera and motion sensors).
REQ-10-25-05-04	A framework service shall be defined allowing the UICC to provide a notification to the end user (e.g. acknowledgement of service usage) by means such as display, audio (e.g. a short melody, a ring tone or a voice message), or vibrating system.
REQ-10-25-05-05	A framework service shall be defined allowing the end-user to launch applications residing in the UICC.
REQ-10-25-05-06	A framework service shall be defined allowing the terminal to integrate the available UICC applications in the end-user interface in the same way as applications having similar categories provided by the terminal (e.g. game applications are displayed in the "Game" menu of the terminal).
REQ-10-25-05-07	The framework service for integration of UICC applications described in REQ-10-25-05-06 shall be based on meta information (e.g. category, visibility, icons and name) to be used by the terminal.
REQ-10-25-05-08	A framework service shall be defined to manage the availability of applications provided by the UICC to the end-user (e.g. visibility, category or name change).
REQ-10-25-05-09	The framework shall provide means for the terminal to indicate to the end-user that an application is provided by the UICC.
REQ-10-25-05-10	A framework service shall be defined allowing the UICC to request the terminal to start an interaction with the end-user (e.g. pop-up or browser page).

4.25.3.6 Device interaction requirements

Identifier	Requirement
REQ-10-25-06-01	A framework service shall be defined allowing the UICC to access local information such as MCC, MNC and IMEI.
REQ-10-25-06-02	A framework service shall be defined allowing the UICC and terminal to request activation/deactivation of UICC interfaces (such as SWP).
REQ-10-25-06-03	Framework services shall be defined allowing the UICC to gain access to terminal peripherals such as GPS, fingerprint sensor, memory device.

4.25.3.7 Network related requirements

Identifier	Requirement
REQ-10-25-07-01	A framework service shall be defined allowing the UICC to query the connectivity state of the terminal (e.g. not connected, connected or level of service).
REQ-10-25-07-02	The connectivity service described in REQ-10-25-07-01 shall be available for every network interface provided by the terminal (e.g. GPRS, 3G, LTE, Wi-Fi, WiMax and Bluetooth[TM]).
REQ-10-25-07-03	A framework service shall be defined allowing the UICC to configure the network access parameters of the terminal.

4.25.3.8 Specific Services requirements

Identifier	Requirement
REQ-10-25-08-01	A framework service shall be provided allowing the UICC to request time services from the terminal (e.g. current time and date, timer activation and expiration, wakeup, and alarm).

4.25.3.9 Backwards compatibility requirements

Identifier	Requirement
REQ-10-25-09-01	When both the terminal and the UICC support CAT as described in ETSI TS 102 223 [2] as well as the new framework, services shall be accessed exclusively through the framework selected by the UICC.
REQ-10-25-09-02	Existing UICC applications using proactive services as defined in ETSI TS 102 223 [2] shall be able to use transparently the new framework even if they are not designed to do so.

4.25.4 Interaction with existing features (informative)

It is envisaged that the following features will be impacted by this new framework:

- Remote Management over IP.

- Confidential Application.

- New Runtime Environment.

- Internet Connectivity.

4.26 Integration of a UICC in a Mobile Broadband Notebook

4.26.1 Abstract (informative)

This clause describes the use cases and requirements related to the integration of a UICC in a Mobile Broadband Notebook (MBNB).

4.26.2 Background (informative)

4.26.2.1 Architecture considerations

ETSI TR 102 906 [i.6] suggests a number of architectures. Figure 6 summarizes these architectures indicating both common and optional connections.
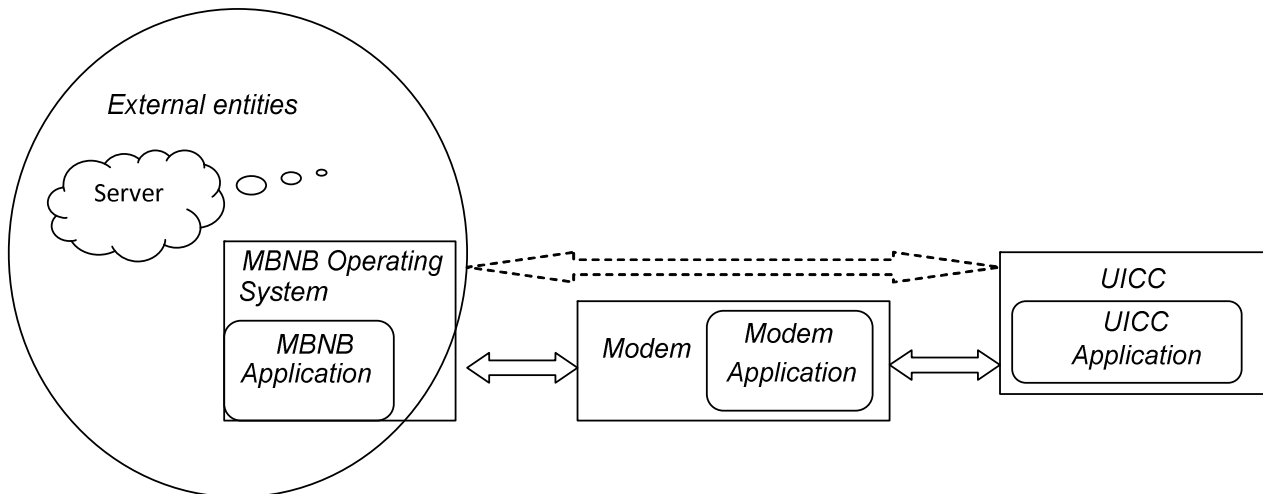
Figure 6: Common and Optional Connections

An MBNB Application is an application running outside the modem (e.g. in the Notebook operating system).

A Modem Application is an application running inside the modem (e.g. Management of the network access).

A UICC Application is an application running inside the UICC (e.g. Network Access Application).

Dotted lines in figure 6 indicate optional connections.

4.26.2.2 Use cases

4.26.2.2.1 Authentication

a) Mobile network authentication:

- When the user wants to use Mobile Broadband with a Mobile Broadband Notebook, the Mobile Modem relies on a UICC to provide authentication with the appropriate Network Access Application (e.g. USIM, CSIM or ISIM).

b) Additional authentication services:

- The UICC can provide additional authentication services as described in the following scenarios:

    ▪ **Scenario 1:** A user can log in to an Internet account (web, email, etc.) and be authenticated using a one-time password generated by the UICC.

    ▪ **Scenario 2:** A user can connect to the Internet through a Wi-Fi access point with a Mobile Broadband Notebook using the UICC EAP PSK TLS authentication provided by the UICC. The user can also be connected to Internet using Mobile Broadband. Considering both solutions, the user can be connected to the Internet using any network technology and according to a defined access priority, e.g. 1st - Wi-Fi access, 2nd - Mobile Broadband, 3rd - other network access.

    ▪ **Scenario 3:** In case IMS services are offered on the MNO network, the UICC can provide authentication based on ISIM application and GBA services. The services could be compliant with RCS recommendation [i.1].

4.26.2.2.2   Mass storage for MNO content

The UICC has mass storage which holds MNO content. This content can be used to personalize the Mobile Broadband Notebook. The content can consist of applications or other data as described in the following scenarios:

Scenario 1: An MNO provides applications in conjunction with the UICC such as:

- Connection managers;

- Voice over IP clients;

- Rich Communication Suite clients; and

- Internet TV players.

Scenario 2: An MNO provides multimedia data such as video and music which may be protected with DRM.

With the UICC, the MNO benefits from an easy means to personalize multimedia applications on the Mobile Broadband Notebook, allowing to port its services on any Mobile Broadband Notebook.

4.26.2.2.3   Mass storage for user content

The UICC has mass storage which holds user content. This storage can be regular storage or secure storage as described in the following scenarios:

Scenario 1: Regular storage can be used for documents, spreadsheets, emails, pictures, phone-books, etc.

Scenario 2: Secure storage can be used for:

- Certificates required for the installation of signed software;

- Certificates required for accessing secure web sites, e.g. banking or personal taxes;

- Applications parameters; and

- Different login credentials for single sign-on mechanisms.

4.26.2.2.4   Cryptographic services

The UICC can be used as a cryptographic coprocessor to the Mobile Broadband Notebook to increase the security as described in the following scenarios:

Scenario 1: The UICC's random number generator can be used to generate session keys, nonces and other security parameters. This service can be used for establishing VPNs or encrypting/decrypting data transmitted from/to the Mobile Broadband Notebook.

Scenario 2: The UICC can be used for digital signature schemes as it can securely store and use private keys (e.g. verifying digital signature on document or application software).

Scenario 3: The UICC can be used to encrypt/decrypt user data such as documents.

4.26.2.2.5   Web services

The UICC can be used to enhance web services as described in the following scenarios:

Scenario 1: The UICC is used to establish a secure channel with a web site that offers banking, tax reporting or other sensitive services.

Scenario 2: The UICC is used to establish a secure channel with the user's home network.

Scenario 3: The UICC hosts a portal used to promote new MNO (or third party) services or applications. The MNO can remotely update its content (html pages, servlets, etc.) through a web connection.

Scenario 4: The UICC hosts a user homepage that is customizable by the user.

4.26.2.2.6 Secure execution environment

The UICC can offer a secure execution environment that is not exposed to the Mobile Broadband Notebook's environment. The secure environment can be managed by the MNO using existing remote management technologies. The secure environment can be used to execute sensitive applications such as banking or tax applications.

4.26.2.2.7 Device Management

Using existing technologies for remote management of the UICC, an MNO can provide application life-cycle management and usage-tracking services for both the UICC and Mobile Broadband Notebook. For example, the UICC can be used to manage MNO rules and parameters for the Connection Manager. This would allow the Connection Manager to be bootstrapped and its roaming and network priorities to be remotely managed.

4.26.2.3 Security considerations

When the UICC is integrated in a Mobile Broadband Notebook, irrelevant of the architecture used, the secure usage and access of UICC services need to be ensured. The following attacks is prevented: a remote application or malware running in the Mobile Broadband Notebook requests sensitive services from the UICC (such as authentication command) without any security check.

In order to prevent such configuration, some rules should be defined allowing the UICC to identify which application originated the service invocation.

The GSMA issued guidelines on the integration of the UICC in Mobile Broadband Notebook (Mobile Broadband in Notebooks Guidelines, version 4.0, December 2009 [i.5]) and has identified a solution based on logical channel filtering combined with the usage of Secure Channel as described in ETSI TS 102 484 [23]. However, the solution described in the GSMA document is based on the existing standard and may prevent some valuable use cases.

> EXAMPLE: If the modem needs to open a second logical channel for IMS authentication, this second logical channel may be filtered by the UICC application, preventing the execution of the IMS authentication.

The requirements below will offer greater flexibility and will allow the modem to use all the required resources in the UICC without compromising the security of the system as identified by the GSMA guidelines.

4.26.3 Requirements

4.26.3.1 Generic requirements

Identifier	Requirement
REQ-10-26-01-01	There shall be a mechanism to inform the UICC if it is inserted in a Mobile Broadband Notebook or in a Terminal, each of which characterized by a software execution environment which allows applications to be loaded and executed.
REQ-10-26-01-02	There shall be a mechanism to inform the UICC if an incoming command has been generated by a modem application or by an external entity.
REQ-10-26-01-03	There shall be a mechanism so that, among the different applications running on external entities sending commands to the UICC, the UICC can differentiate the source of the command.
REQ-10-26-01-04	The mechanisms required in REQ-10-26-01-02 and REQ-10-26-01-03 shall be defined for both the interfaces defined in ETSI TS 102 221 [1] and in ETSI TS 102 600 [24].

4.26.3.2 Security requirements

Identifier	Requirement
REQ-10-26-02-01	There shall be a mechanism for the UICC and/or the application running on the UICC to apply different security policies (e.g. usage of the secure channel or not), depending on the source (e.g. modem or external entity) and the type of the command (e.g. Authenticate command is not allowed for external entities without usage of a secure channel).
REQ-10-26-02-02	There shall be a mechanism to allow applications running in the UICC to authenticate applications running on external entities.
REQ-10-26-02-03	There shall be a mechanism to protect the integrity of the data exchanged between an application running in the UICC and an application running in an external entity.
REQ-10-26-02-04	There shall be a mechanism to protect the confidentiality of the data exchanged between an application running in the UICC and an application running in an external entity.
REQ-10-26-02-05	There shall be a mechanism for a UICC application to close the communication channel between an application running on an external entity and that application running on the UICC.
REQ-10-26-02-06	There shall be a mechanism to establish and maintain an initial communication channel reserved for modem applications (e.g. Logical channel 0).

4.26.3.3 Security policy related requirements

Identifier	Requirement
REQ-10-26-03-01	There shall be a uniform way of describing the security policy to be applied by the UICC.
REQ-10-26-03-02	This security policy shall be defined on an application basis for first level applications.
REQ-10-26-03-03	There shall be a mechanism available allowing changes to the security policy of an application.

4.26.4 Interaction with existing features (informative)

The implementation specified to fulfil the above requirements may impact the Secure Channel as described in ETSI TS 102 484 [23] and the CAT access over the modem interface feature.

4.27 Fourth UICC Form Factor

4.27.1 Abstract (informative)

There is a growing market trend for smaller, slimmer mobile devices. This trend has created a need for a smaller UICC form factor since the existing form factors are limiting the ability of device manufacturers to either minimize the physical size of the devices or add features to existing designs.

The Fourth UICC Form Factor (4FF) as defined will be smaller than the current Mini-UICC, retain existing UICC functionalities as specified in the ETSI specifications and be backwards compatible to existing UICC form factors specified in ETSI TS 102 221 [1]. No changes to the electrical specifications are anticipated.

4.27.2 Background (informative)

4.27.2.0 General

Below are some use cases that relate to the Fourth UICC Form Factor.

4.27.2.1 Use Case - Introduction of new devices that can support UICC

The smaller form factor of 4FF will allow device manufacturers to use the UICC in devices that are space constrained. For e.g. personal health monitoring devices such as devices tied to users arm that measures distance travelled, etc.

4.27.2.2 Use Case - Slimmer mobile devices

Since 4FF is physically smaller and possibly thinner than its predecessors, 4FF can enable device manufacturers to make slimmer and sleeker mobile devices.

4.27.2.3 Use Case - Enhanced end user experience

Since 4FF is physically smaller than its predecessors,4FF can free up much needed board space within mobile devices that use UICCs. This space can be used to either accommodate bigger batteries or add additional components that enable new functionality. As devices get smarter their power requirements also increase. Increased battery capacity could result in an enhanced user experience along with the enablement of new functionalities.

4.27.3 Technical Solution Selection Criteria

The following selection criteria is to be used when selecting a technical solution in case several technical solutions meet the requirements specified in the present document.

- A preference is to be given to a technical solution for the 4FF that provides an overall space saving, including the mechanical reader, compared to a solution where the UICC size reduction is higher but the size reduction including the mechanical reader is less.

- In case of several solutions providing similar size reduction a preference is to be given to a solution based on the existing plugin/mini UICC contact layout (size and arrangement) compared to a solution based on a different contact layout.

- In case of several solutions providing similar size reduction a preference is to be given to a solution with a shorter time to market than a solution with a longer time to market. Time to market includes availability of both UICCs and mechanical readers.

- A technical solution that prevents "electrical damage" in case of wrong insertion is to be given a preference compared to a solution not providing such protection.

4.27.4 Requirements

Identifier	Requirement
REQ-11-27-01-01	The fourth UICC form factor shall be at least 25 % smaller as compared to the Mini-UICC.
REQ-11-27-01-02	The fourth UICC form factor should be 40 % smaller as compared to the Mini-UICC.
REQ-11-27-01-03	The fourth UICC form factor shall specify 8 contacts.
REQ-11-27-01-04	The usage of the 8 contacts of the fourth UICC form factor shall be compliant with ETSI TS 102 221 [1], clause 4.5.
REQ-11-27-01-05	The fourth UICC form factor shall retain all existing UICC functionalities as specified in the existing ETSI specifications.
REQ-11-27-01-06	It shall be possible to have a legible identifier (e.g. at least ICCID) on a UICC complying to the fourth UICC form factor.
REQ-11-27-01-07	The fourth UICC form factor shall be easily removable and replaceable by the end user (i.e. without requiring specific tools).
REQ-11-27-01-08	The design of the fourth UICC form factor shall prevent the 4FF from becoming jammed in a Mini-UICC reader. An example is that if the 4FF is turned 90 degrees and it fits perfectly into the Mini-UICC reader (4FF length = Mini-UICC width).
REQ-11-27-01-09	The need for an orientation mark to prevent wrong insertion (4FF into 4FF reader) should be considered in order to prevent "electrical damage" of the UICC.
REQ-11-27-01-10	There shall be a maximum contact pad size defined in order to prevent the contact pad metal to stretch to the 4FF card edge (e.g. min. 0,2 mm clearance towards the edge).

4.28 Name resolution mechanism for the UICC

4.28.1 Abstract (informative)

When using a data packet bearer, there is a need to define a new way to connect UICC client applications to server applications by using a domain name instead of an IP address. The resolution of this name needs to be handled using a DNS resolver.

4.28.2 Use Cases (informative)

4.28.2.0 General

Mobile Network Operators or third parties may want to use address resolution instead of fixed IP address for the following services, e.g.:

- Access to an OTA server.

- Access to a payment transaction server.

4.28.2.1 Use Case - Card OTA management

In the context of remote management of a UICC over HTTP, the Mobile Network Operator may want to have some flexibility in the network supporting the remote management servers. The following specific cases could then be addressed:

- The remote management server is moved from one location to another. This implies a modification of the address of the sever.

- The remote management service is subcontracted to a third party. This third party may change during the life time of the UICC, implying a change in the IP address of the server.

- The MNO's network infrastructure is modified. For example by moving from IPv4 to an IPv6 network.

- Several servers may be operating in parallel. Round robin DNS is used to balance the load between these different servers.

4.28.2.2 Use Case - Access to a payment server

A third party payment application is loaded on the UICC. This application wants to access a server on the Internet in order to validate a payment, reload a purse or make some update on some parameters. This application has no knowledge of the network infrastructure and will not request a specific APN.

For such an application provider, details of network are completely out of scope and the only way to reach the server is by using its domain name.

4.28.3 Requirements

Identifier	Requirement
REQ-12-28-01-01	There shall be a UICC mechanism allowing an application to use a domain name to establish an IP connection.
REQ-12-28-01-02	When using the mechanism specified above, applications shall be informed of the following events: • The address resolution is not successful due to a lack of answer from the DNS server or a DNS protocol error. • The address resolution is successful but the DNS server does not return a valid IP address. • The address resolution is successful but the connection to the server is not successful.
REQ-12-28-01-03	This mechanism shall be available on any type of IP network (e.g. IPv4 or IPv6).
REQ-12-28-01-04	In case of both IPv6 and IPv4 address are available for a given domain name, priority shall be given to IPv6.
REQ-12-28-01-05	This mechanism shall not require the use of a new or multiple APN by the terminal.
REQ-12-28-01-06	The Java Card API shall allow for applications to use the mechanisms specified above.

4.28.4 Interaction with existing features (informative)

None.

4.29 UICC Access Optimization

4.29.1 Abstract (informative)

The UICC platform was designed for multiple applications support. While this platform was often used for a single application in the past, it is more and more frequent that multiple applications reside on the UICC (e.g. USIM, ISIM and CSIM). Current and future work in other technical committees and organizations may create further applications and services that may be hosted on the UICC. As the number of applications and services on the UICC grows, the time for the terminal to initialize the UICC and access its content will increase, which in turn affects the user experience. This clause specifies the requirements for UICC access optimization.

4.29.2 Background (informative)

As more applications are added into UICC, the current UICC initialization takes longer and longer time, which affects the user experience significantly. Based on analysis of the UICC interface, optimization on the UICC interface, e.g. for the reading of EFs, will help shorten the UICC initialization time and improve the user experience significantly.

4.29.3 Requirements

Identifier	Requirement
REQ-12-29-01-01	There shall be a mechanism to enhance the reading, processing and transfer of data between the UICC and a Terminal.

4.30 Mechanism for monitoring the wear of a UICC

4.30.1 Abstract (informative)

In the M2M context, it is useful to be able to monitor remotely the wear of a UICC upon its non-volatile memory and to present this information to the user/manager of the M2M devices.

Knowing this information, in conjunction with the characteristics of the UICC (capabilities of the memory, type of area where the file is stored e.g. high reliable area or not), can help evaluating the time ahead the UICC can work correctly.

Such information could also provide a means to detect possible defects in the implementation of a modem or an applet, for example in case an abnormal usage of the UICC.

4.30.2 Use cases (informative)

4.30.2.1 Use case - Remote management of wear index information

A trucks company has installed communication modules into its trucks for providing connected services to the trucks through mobile networks. The communication modules are equipped with a UICC which can be reached through OTA.

The trucks company connects sometimes to its UICCs in the field in order to read the information about the wear index of the UICC non-volatile memory.

The company can then evaluate the time ahead the UICCs can work properly, referring to this information and to the characteristics of the UICCs (capabilities of the memory, type of area where the file is stored e.g. high reliable area or not), provided by the manufacturers of the UICCs. Some of these characteristics may be directly accessible as information stored in the UICC, which might ease some data collection and error detection automated systems.

4.30.2.2 Use case - New communication modules in cars

A company has installed communication modules into cars for providing connected services in the cars through mobile networks. The communication modules are equipped with a UICC which can be reached through OTA.

The company uses the OTA platform to reach the first 1 000 modules released in the field (built-up in the new cars). The OTA platform reads the information about the wear index on the non-volatile memory.

The company can detect a possible defect in the modules implementation in case this information is abnormal.

4.30.2.3 Use case - Automatic detection of memory defects

Some communication modules are equipped with an UICC which can be reached through OTA, providing the capability to get the status of the UICC memory.

Thanks to an internal application stored in the UICC, an OTA platform is capable to collect alerts on defect detection, and the company in charge of managing the UICC is able to take the appropriate actions before the UICC component fails.

4.30.3 Requirements

Identifier	Requirement
REQ-13-30-01-01	The UICC should support a mechanism allowing a remote entity, the terminal and Java Card application to monitor an index (e.g. percentage and/or counter value) about the wear of its non-volatile memory.
REQ-13-30-01-02	The UICC shall be able to indicate if the mechanisms described in REQ-13-30-01-01 has been implemented.

4.31 Mechanism to suspend the UICC

4.31.1 Abstract (informative)

Power consumption is a very critical aspect for many M2M devices, where it is impossible or impractical to recharge or replace the batteries. For this reason, it is desirable to minimize the overall power consumption of the terminal.

The UICC contributes to the overall power consumption. Even if the power absorbed by the UICC when it is in idle state is low (maximum of 100 µA as specified in ETSI TS 102 221 [1]), the overall energy over long periods of time becomes significant. Many M2M devices have only sporadic communication with the network. So, it is desirable to eliminate the power consumption caused by the UICC, when this is not used for long periods of time.

4.31.2 Use cases (informative)

Several use cases where reduction of power consumption is required are described in 3GPP TR 131 970 [i.7] clause 4.

4.31.3 Requirements

4.31.3.1 Power requirements

Identifier	Requirement
REQ-14-31-01-01	There shall be a mechanism allowing the Terminal to suspend the UICC (e.g. remove the power from the UICC) for a certain duration and to restore the UICC to the state it was in before being suspended.
REQ-14-31-01-02	The mechanism shall be triggered by the terminal, if supported by the UICC.
REQ-14-31-01-03	The UICC shall be able to postpone or reject the usage of the mechanism.
REQ-14-31-01-04	The terminal and the UICC shall be able to negotiate the duration of the suspension.

4.31.3.2 Toolkit requirements

Identifier	Requirement
REQ-14-31-02-01	The mechanism shall allow the toolkit applications in the UICC to be restored.
REQ-14-31-02-02	The mechanism shall not interrupt ongoing BIP sessions initiated by the UICC
REQ-14-31-02-03	The mechanism shall not interrupt an active proactive UICC session.
REQ-14-31-02-04	The mechanism shall not prevent the UICC from receiving any event for which it has registered (SET UP EVENT LIST command, TIMER MANAGEMENT command, ...).

4.31.3.3 Security requirements

Identifier	Requirement
REQ-14-31-03-01	The mechanism shall include security features that give it a security level equivalent to the PIN verification mechanism.
REQ-14-31-03-02	The mechanism shall ensure that the UICC can only be resumed by the Terminal that suspended it.
REQ-14-31-03-03	The level of security in suspended mode shall be equivalent to the level of security in powered-off mode.
REQ-14-31-03-04	The UICC shall discard any saved state information in the absence of a resume attempt (e.g. Terminal not supporting the mechanism) or in case the security conditions defined in this section are not fulfilled during a resume sequence.

4.31.3.4 Backward compatibility requirements

Identifier	Requirement
REQ-14-31-04-01	The mechanism shall not prevent the usage of a UICC supporting it in a terminal that does not support it.
REQ-14-31-04-02	The support of the new mechanism by the UICC shall be indicated to the Terminal. The mechanism shall allow a terminal that supports it to use a UICC that does not support it.
REQ-14-31-04-03	The resume sequence shall comply with the initial communication establishment procedures specified in ETSI TS 102 221 [1].

4.32 UWB services

4.32.1 Abstract (informative)

The UWB radio technology allows the implementation of ranging systems allowing localizing precisely objects even in in-door environments where no geo localization services are working. For secure applications the UWB technology offers also a secure ranging mechanism preventing relay attacks according [29]. This technology allows additionally the exchange of data.

4.32.2 Background (informative)

4.32.2.1 General

This clause lists use cases relevant for UWB Services.

Implementing UWB services in the mobile and in a secure element, like the UICC, enhances the user experience, for example by adding MMI capabilities, enables remote administration of these services (application download, personalization, administration, etc.) and provides the required security.

4.32.2.2 Use case - retail

The customer can enable on his/her mobile device the payment on the go function when entering a shop. When the customer is near by the cashier, he is only confirming the payment of the bought products by confirming his purchase at a customer terminal. Therefore, the customer does not need to put his/her phone or credit card out of the pocket to perform the payment. The UICC contains the necessary credentials for the payment transactions.

4.32.2.3 Use case - transport

The traveller can enable on his/her mobile phone the ticket on the go function when entering the gates of public transport systems. These gates register the travellers entering and leaving the public transport gates to calculate and bill their transport fare. The traveller does not need to pick their mobile phone or transport ticket when passing the gates. Such a system increases the throughput of the entrance gates. The UICC contains the necessary credentials of the transport ticket.

4.32.2.4 Use case - automotive

In case of use of virtual car keys stored inside the UICC, the UWB enables keyless entry use cases: when the user gets near the car it starts flashing some lights, when he gets near enough the doors are unlocked (the system can even precisely open the door in front of the user), when he gets inside the car the engine can be started.

The UICC performs the necessary authentications to lock/unlock the door and to start the engine.

4.32.2.5 Use case - object tracking

The users owning several portable devices with UWB can enable the UWB technology to find these devices with his mobile phone when he/she does not remember where he/she has located these devices inside their home. To avoid tracking by unauthorized persons, this localization function will be only available for the owner of the portable devices. The UICC contains the necessary credentials to verify a search by the owner of the portable device.

4.32.2.6 Use case - building access

Keys to access buildings can be stored inside the UICC. When an employee enters nearby the entrance door of his company the employee will be localized and identified by UWB technology and opens automatically the entrance door without the need for the employee to show his/her badge.

The user can install at home a door lock system which identifies with UWB technology the user and unlocks automatically the entrance door when the user is nearby.

The UICC contains the necessary credentials for the building access.

4.32.2.7 Use case - ticketing

A visitor can enable on his mobile device a ticket on the go feature when entering an event. At the entrance gate the visitor will be automatically identified and get the allowance to pass the entrance gate without the need to show the ticket or the mobile phone with the ticket. Such a system increases the throughput of the entrance gates. The UICC stores the credentials of the ticket.

4.32.3 Requirements

Identifier	Requirement
REQ-16-32-01	The UWBC shall be accessible from the UICC.
REQ-16-32-02	The link between the UICC and the UWBC shall provide a way to know and control the configuration of the UWB PHY layer according [28] and [29].
REQ-16-32-03	The link between the UICC and the UWBC shall have the means to exchange data payload via the UWB MAC layer according [28].
REQ-16-32-04	The link between the UICC and the UWBC shall be able to enable the secure ranging mechanism to prevent relay attacks.
REQ-16-32-05	The UWBC shall be capable of providing the UICC with UWBC state (e.g. if UWBC is in use or not).
REQ-16-32-06	The UWBC should be able to provide the latest ranging result as well as the period of time since this measure was done and to inform if the secure ranging mechanism according [29] was activated at time of measure.
REQ-16-32-07	The UICC shall be able to require a periodic ranging procedure with a given frequency from the UWBC.
REQ-16-32-08	The UWBC shall provide a way for the UICC to configure the security services for the MAC layer according [28].
REQ-16-32-09	The UWBC shall provide a way for the UICC to provide the keys needed to reach expected security level (both communication and ranging) as defined in [28].
REQ-16-32-10	There shall be a means to prevent conflicts when the UWBC is shared between UICC and the terminal.
REQ-16-32-11	There shall be a mechanism for creating secure connections between the UWBC and the UICC.
REQ-16-32-12	UWBC and UICC may support the mechanism defined in REQ-16-32-11
REQ-16-32-13	The secure connection defined in requirement REQ-16-32-11 shall provide confidentiality, integrity and replay protection.
REQ-16-32-14	There shall be a means, e.g. API, on the UICC to support the secure mechanism defined in requirement REQ-16-32-11.
REQ-16-32-15	The secure mechanism defined in requirement REQ-16-32-11 shall support the transport of all keys required by the UWBC.

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-29	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-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-080455	8.2.0	028	1	B	Introduction of DVB location information usecases and requirements	8.3.0
	SCP-080479	8.2.0	029	1	F	Clarification of availability of proactive handler for SCWS applications	8.3.0
	SCP-080456	8.2.0	030	1	B	Requirements for the identification of terminals with reduced functionality	8.3.0
	SCP-080476	8.2.0	031		B	Addition of Secure Removable Media on UICC requirements (renumbered from 24r2 to 31)	8.3.0
	SCP-080452	8.3.0	026	2	B	Introduction of multicast dataflow usecases and requirements	9.0.0
SCP-40	SCP-090056	9.0.0	032		F	Correction of requirements for Confidential Applications (Rel-9 implementation based on Rel-8 CR)	9.1.0
SCP-41	SCP-090155	9.0.0	035		C	Modification of requirement REQ-8-17-04-05 to remove method level access policy for Third Party Applications	9.1.0
	SCP-090174	9.0.0	033	1	B	Use cases and requirements for new data storage and access	9.1.0
	SCP-090175	9.0.0	036		B	Enhanced security for third party administration	9.1.0

Meeting	Plenary Tdoc	Old Version	CR	REV	CAT	SUBJECT	Resulting Version
SCP-42	SCP-090244	9.1.0	037		B	One click menu for the UICC	9.2.0
	SCP-090266	9.1.0	038	1	B	Addition of requirements for long scripts and online mode	9.2.0
SCP-44	SCP(10)0092	9.1.0	039	2	B	Addition of Use cases and requirements for CAT access on Modem interface	9.2.0
SCP-43	SCP-090339	9.2.0	040		B	Support of RFID services	10.0.0
	SCP-090360	9.2.0	041	1	B	Introduction of use cases and requirements for a new framework for application and services over USB	10.0.0
SCP-44	SCP(10)0094	9.2.0	043	1	B	New security requirements for the CAT over AT feature	10.0.0
	SCP(10)0093	9.2.0	044	1	C	Allowing multiple connected entities for CAT over AT	10.0.0
SCP-45	SCP(10)0158	10.0.0	045	-	B	Addition of a requirement for expanded support of large HTTP messages in SCWS API (ETSI TS 102 588)	10.1.0
	SCP(10)0159	10.0.0	046	-	B	Introduction of requirements for a selective secure channel able to handle toolkit commands	10.1.0
SCP-46	SCP(10)0302r2	10.1.0	048	2	B	Use cases and security Requirements for the integration of a UICC in a Mobile Broadband Notebook	10.2.0
SCP-47	SCP(11)0070r1	10.2.0	049	1	C	Clarification of requirements for Secure Channel able to handle toolkit commands	10.3.0
SCP-48	SCP(11)0132	10.3.0	050	-		CR 102 412 R11 #050: Use cases and requirements for Contactless power negotiation	11.0.0
SCP-48	SCP(11)0133r1	10.3.0	051	1	B	New peer to peer use cases and requirements	11.0.0
SCP-52	SCP(11)0268r2	11.0.0	052		B	Use cases and requirements related to Fourth UICC Form Factor	11.1.0
SCP-53	SCP(11)0391	11.1.0	053		C	Alignment of requirements for secure channel for CAT and CAT over the modem interface	11.2.0
SCP-55	SCP(12)000132	11.2.0	054		B	Addition of requirements to support DNS for BIP	12.0.0
SCP-60	SCP(13)000184r1	11.2.0	055	1	B	Addition of a requirement to store information of environmental classes in an M2M UICC	12.0.0
SCP-62	SCP(14)000072	11.2.0	056		B	Addition of requirement about terminal s user interface availability	12.0.0
SCP-63	SCP(14)000124r1	11.2.0	057	2	B	Addition of use cases and requirements to answer interoperability issues between the UICC and other potential contactless Execution Environment	12.0.0
SCP-63	SCP(14)000123r1	11.2.0	058	1	B	Requirements for UICC File Access Optimization	12.0.0
SCP-67	SCP(15)000055r1	12.0.0	59	1	B	Uses case and requirements for a mechanism for monitoring the wear index of the UICC	13.0.0
SCP-67	SCP(16)000082	12.0.0	60	1	B	Use cases and requirements for a mechanism to suspend the UICC	14.0.0
						Automatic Upgrade	15.0.0
SCP-92	SCP(20)000014r1	14.0.0	63		B	Requirements on support of UWB services	16.0.0

History

Document history		
V16.0.0	July 2020	Publication