ETSI TS 102 412 V7.1.0 (2005-11)

Technical Specification

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

Reference

RTS/SCP-R00002R1

Keywords

smart card

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

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

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

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

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

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI Project Smart Card Platform (SCP).

The contents of the present document are subject to continuing work within TC SCP and may change following formal TC SCP approval. If TC SCP modifies the contents of the present document, it will then be republished by ETSI with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

0 early working draft;

1 presented to TC SCP for information;

2 presented to TC SCP for approval;

3 or greater indicates TC SCP approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

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

1 Scope

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

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

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to an TC SCP document, a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

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

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

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

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

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

[5] ETSI TS 131 102: "Universal Mobile Telecommunications System (UMTS); Characteristics of the USIM application (3GPP TS 31.102 version 6.11.0 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 Design Principles" specification version 1.2.

NOTE: Available at https://www.trustedcomputinggroup.org/downloads/tpmwg-mainrev62_Part1_Design_Principles.pdf.

3 Definitions, symbols, abbreviations and coding conventions

3.1 Definitions

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

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

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 were applicable, in case this distinction is not relevant the generic term terminal will be used.

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

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

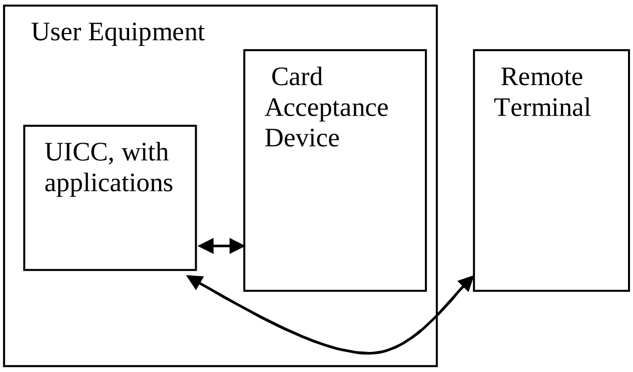

Figure 1: Possible secure channels with a UICC

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.

3.2 Symbols

Void.

3.3 Abbreviations

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

ADF	Application Dedicated File
CAT	Card Application Toolkit
CAD	Card Acceptance Device
CEK	Content Encryption Key
DF	Dedicated File
DRM	Digital Rights Management
DRM_UA	Digital Rights Management User Agent
EF	Elementary File
IP	Internet Protocol
IMS	IP Multimedia Services
ISIM	IMS SIM
JSR	Java Specification Request
ME	Mobile Equipment
MNO	Mobile Network Operator
MT	Mobile Termination
OMA	Open Mobile Alliance
PIN	Personal Identification Number
POP	Post Office Protocol
RO	Rights Object
SMTP	Simple Mail Transfer Protocol
TCG	Trusted Computing Group
TMP	Trusted Media Player
UMTS	Universal Mobile Telecommunications System
UE	User Equipment
URL	Uniform Resource Locator
USIM	Universal Subscriber Identity Module
WIM	Wireless Identity Module

3.4 Coding Conventions

Void.

4 Requirements

The present document specifies:

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

4.1 Run time environment timing constraints

4.1.1 Abstract (informative)

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

4.1.2 Background (informative)

4.1.2.1 Use case - Network authentication

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

4.1.3 Requirements

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

4.1.4 Interaction with Existing Features (informative)

(none)

4.2 Launch Application command

4.2.1 Abstract (informative)

(none)

4.2.2 Background (informative)

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

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

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

Example of terminal applications for such a feature:

- E-mail:

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

- Network management optimization:

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

- Proactive synchronization:

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

- Streaming:

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

4.2.3 Requirements

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

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

Depending on the terminal application A:

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

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

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

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

4.2.4 Interaction with Existing Features (informative)

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

Other pre-release 7 features should not be impacted.

4.3 Mapped file support on the UICC

4.3.1 Abstract (informative)

(none)

4.3.2 Background (informative)

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

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

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

4.3.3 Requirements

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

4.3.4 Interaction with Existing Features (informative)

(none)

4.4 Extension of logical channels

4.4.1 Abstract (informative)

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

4.4.2 Background (informative)

4.4.2.1 Typical problem situation

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

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

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

4.4.2.2 Possible problem solution

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

4.4.2.3 Use cases

Use case 1: JSR 177 applications

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

Use case 2: PC connection

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

4.4.3 Requirements

4.4.3.1 General Requirements

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

4.4.3.2 Backward compatibility requirements

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

4.4.4 Interaction with existing features (informative)

(none)

4.5 Secure channel to secure local terminal interfaces

4.5.1 Abstract (informative)

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

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

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

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

4.5.2 Background (informative)

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

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

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

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

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

Multiple use cases justify the need for a smart card to terminal secure communication. In the following parts, we cover use cases linked with User Interface, Device Management, Digital Right Management.

4.5.2.1 Use case: User Interface

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

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

- When an application on the UICC requires the user to enter a PIN to access a service, the PIN itself is not protected. Therefore, when PIN data is sent from the handset to the UICC, it may be stolen or maliciously altered in order to deny the service to the end user.

- When an application on the UICC sends data to the terminal to display to the user, the data is displayed in plain text. Such data may involve, for example, fees to be paid or acceptance of onerous conditions for the use of a software/service. If data is tampered with, the user may take upon him/herself a burden different from that which has been notified. Issues may be raised on how "legally binding" for a user is the acceptance of conditions that have no protection against malicious alteration before submission to the user itself.

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

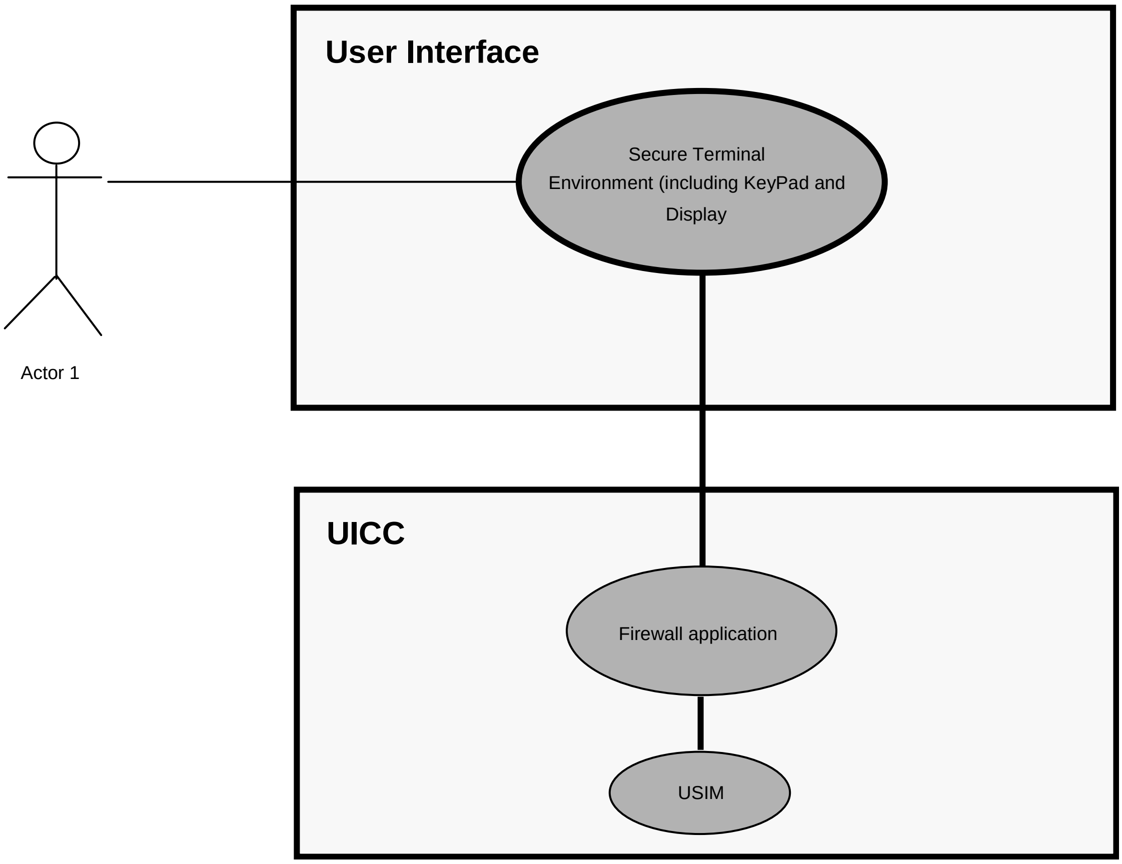

Figure 2: User Interfaces

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

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

- Setting initial configuration information in devices.

- Subsequent installation and updates of persistent information in devices (firmware update).

- Retrieval of management information from devices.

- Processing events and alarms generated by devices.

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

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

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

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

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

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

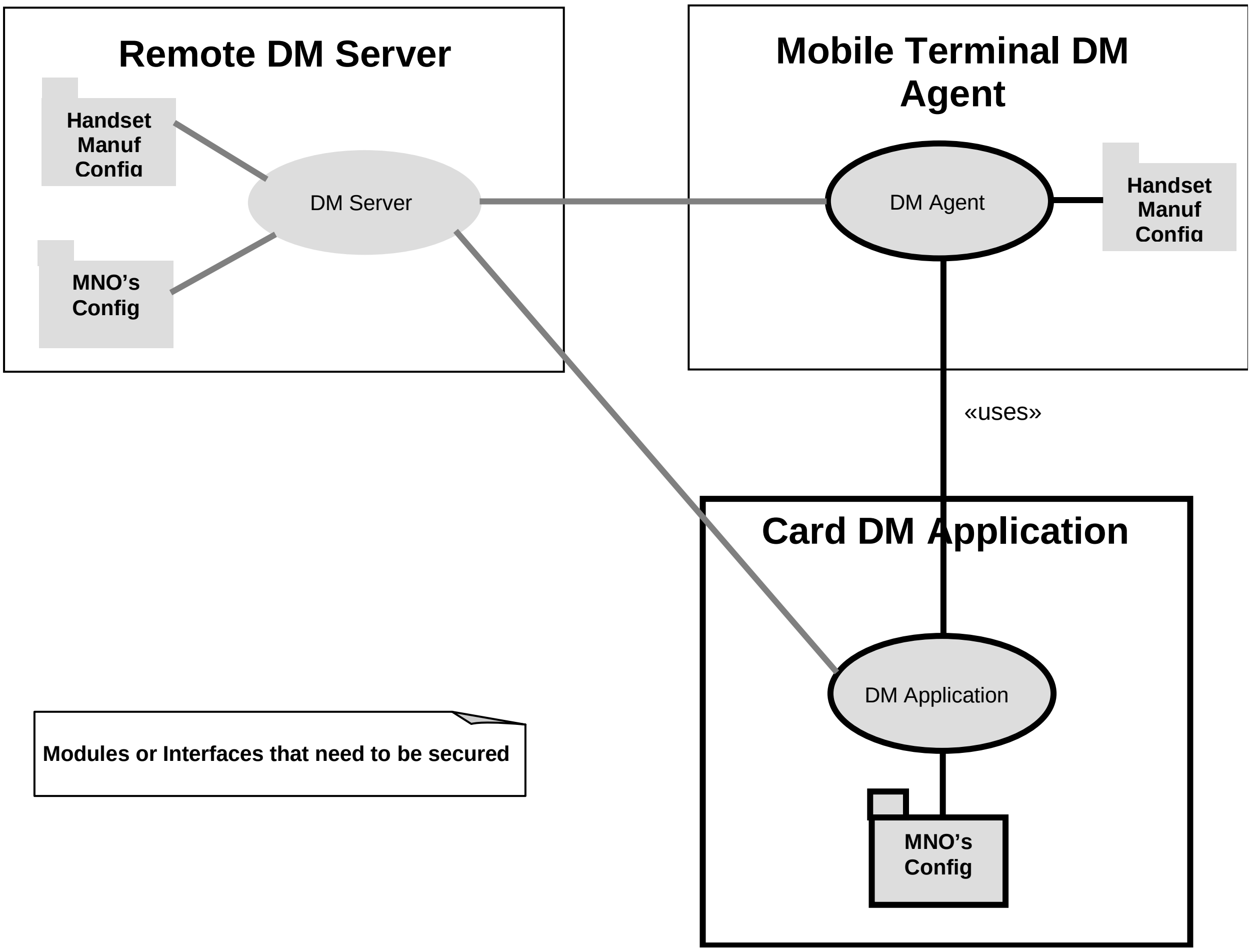

Figure 3: Device Management

4.5.2.3 Use case: DRM and distributed applications

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

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

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

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

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

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

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

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

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

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

Then the TMP can play the content.

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

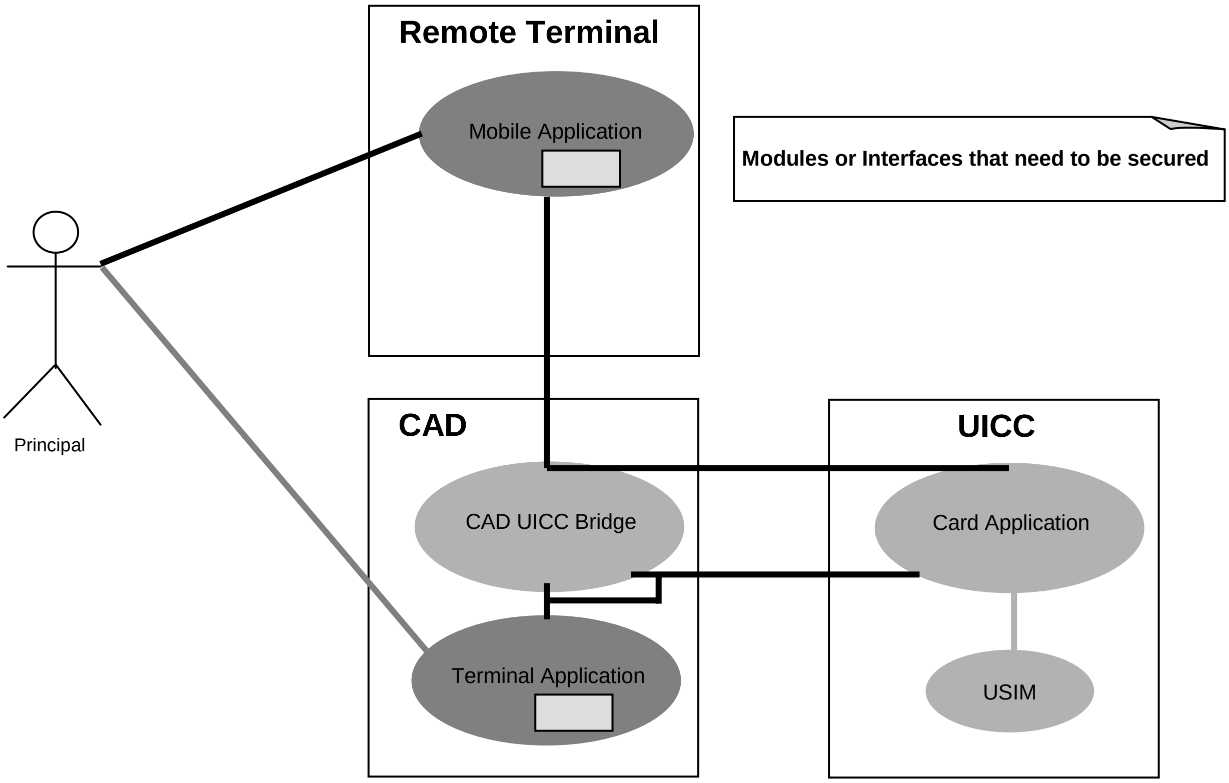

Figure 4: Distributed Application

4.5.3 Requirements

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

4.5.3.1 End point Requirements

Identifier	Requirement
REQ-7-0x-01-01	The UICC shall be able to establish a secure channel with 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.x.2.1, 4.x.2.2, 4.x.2.3).

4.5.3.2 Integrity Requirements

Identifier	Requirement
REQ-7-0x-02-01	The secure channel shall allow the integrity of the data to be verified (see use cases in clauses 4.x.2.1, 4.x.2.2, 4.x.2.3).

4.5.3.3 Confidentiality Requirements

Identifier	Requirement
REQ-7-0x-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.x.2.1, 4.x.2.2, 4.x.2.3).

4.5.3.4 Authentication Requirements

Identifier	Requirement
REQ-7-0x-04-01	It shall be possible for the UICC to authenticate itself to any Terminal end point compliant with this feature (see use cases in clauses 4.x.2.1, 4.x.2.2).
REQ-7-0x-04-02	It shall be possible for a Terminal end point to authenticate itself to any UICC compliant with this feature (see use cases in clauses 4.x.2.1, 4.x.2.3).

4.5.3.5 Audit/Compliance Requirements

Identifier	Requirement
REQ-7-0x-05-01	The terminal end point shall be a trusted device (see clause 4.x.2).
REQ-7-0x-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.x.2).

4.5.3.6 Policy Requirements

Identifier	Requirement
REQ-7-0x-06-01	An anti-replay mechanism shall be present and active depending on the policy.
REQ-7-0x-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.
REQ-7-0x-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 that has authenticated itself to the terminal.

4.5.4 Interaction with existing features (informative)

(none)

Annex A (informative): Change history

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

Meeting	Plenary Tdoc	Old Version	CR	REV	CAT	SUBJECT	Resulting Version
SCP #21	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

History

Document history		
V7.0.0	September 2005	Publication
V7.1.0	November 2005	Publication