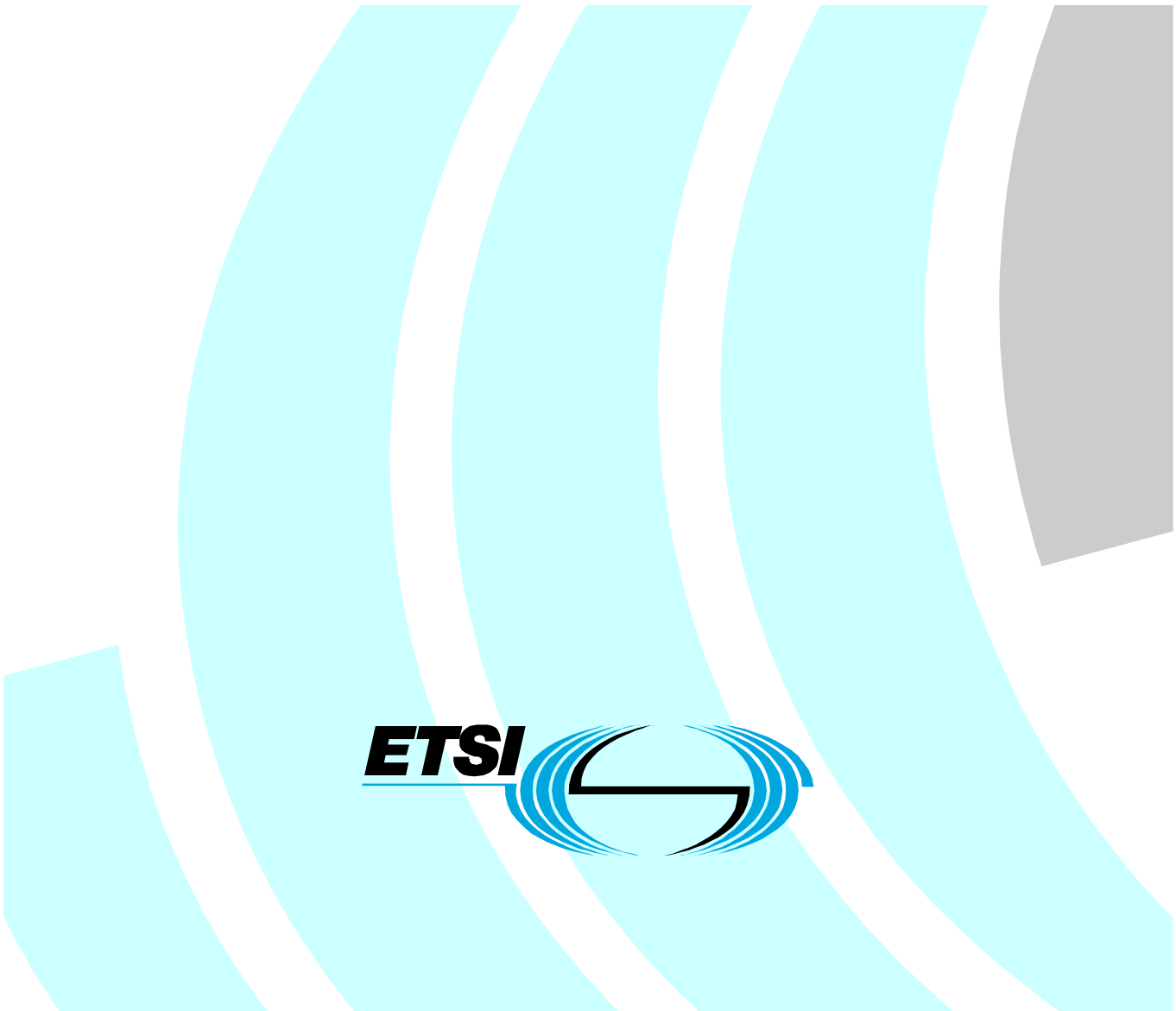
# ETSI TS 102 266 V7.1.0 (2006-01)

*Technical Specification*

**Smart Cards;**
**USSM: UICC Security Service Module;**
**Stage 1**



Reference
RTS/SCP-R0002r1

Keywords
smart card, security

***ETSI***

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

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

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

# Contents

# Intellectual Property Rights

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

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

# Foreword

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

The present document defines the stage 1 description for the USSM.

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

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

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

# 1 Scope

The present document describes the functional requirements of the USSM, a generic UICC Security Service Module, to be used by the applications on an UICC. It defines the necessary framework for supporting and managing the USSM on an UICC.

The concept of the USSM is flexible enough to allow additional security objects and operations to be added easily in later versions of the specification or during the specification of a stage-2 document.

# 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 a EP 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] ISO 16609: "Banking - Requirements for message authentication using symmetric techniques".

[2] ISO/IEC 9796-2: 2002: "Information technology - Security techniques - Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms".

NOTE: See ISO/IEC 9796-2:2002

[3] OMA-WAP-WIM-V1-2-20050322-C, Wireless Identity Module, Version 1.2 - 22 March 2005 .

# 3 Definitions and abbreviations

## 3.1 Definitions

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

**access attributes:** access conditions associated to a sensitive object

**authentication object:** PIN or a key for a challenge response mechanism that is used for authentication purposes

**card issuer:** entity that owns the card

**DES:** Data Encryption Standard, standard cryptographic algorithm specified as DEA in ISO 16609 [1]

**digital signature:** message digest of the document encrypted with the secret signing key of the signer, along with information about the signer and the algorithms used

**information attributes:** informational data associated to a sensitive object

**sensitive object:** data object containing sensitive and/or protected information like keys, pins or certificates. Most objects on the USSM are sensitive and have to be protected against unauthorized access

NOTE: The term might also include objects, which are not sensitive (e.g. some user certificates might be not sensitive), but are handled by the USSM in the same manner.

**USSM owner:** entity that controls the USSM and has the right to administer its objects

NOTE: It can be the card issuer, but also an application provider

## 3.2 Abbreviations

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

| | |
|---|---|
| AA | Access Attributes |
| API | Application Program Interface |
| DES | Data Encryption Standard |
| DF | Directory File |
| DRM | Digital Rights Management |
| DSA | Digital Signature Algorithm |
| IA | Information Attributes |
| OTA | Over the Air |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| RSA | Rivest / Shamir / Adleman asymmetric algorithm |
| SO | Sensitive Object |
| USSM | UICC Security Services Module |
| WIM | Wireless Identity Module |

# 4 Introduction and Overview

## 4.1 Introduction

The USSM is a general security module on the UICC, which offers security services to applications on the UICC through an API with standardized functions. The USSM can store sensitive data and manage access to sensitive data. Different applications could use different keys, but through access mechanisms it is also possible to share keys, especially when using PKI technology.

Possible areas where the USSM adds value are authentication, signatures, DRM, secure EMail, payments, banking, application download (to the card and terminal device) etc. Besides the advantage in having a generic API towards the security objects it also could be beneficial in reducing the space needed for each application using its own APIs and keys.

Through a kind of proxy application it is also possible to offer services of the USSM to entities outside the UICC, e.g. the Mobil Equipment or the network. The requirements of the interface of this proxy application (which can be used by entities outside the card) is not part of the present document.

This version of the stage 1 specification focuses on the most common sensitive objects and operations. Other features like key agreement, key wrapping, DSA, and support for additional encryption and decryption schemes may be added in later versions, depending on future requirements and appropriate support.

## 4.2 Overview

The following figure shows the logical components of the USSM and various sample applications that may use the USSM.

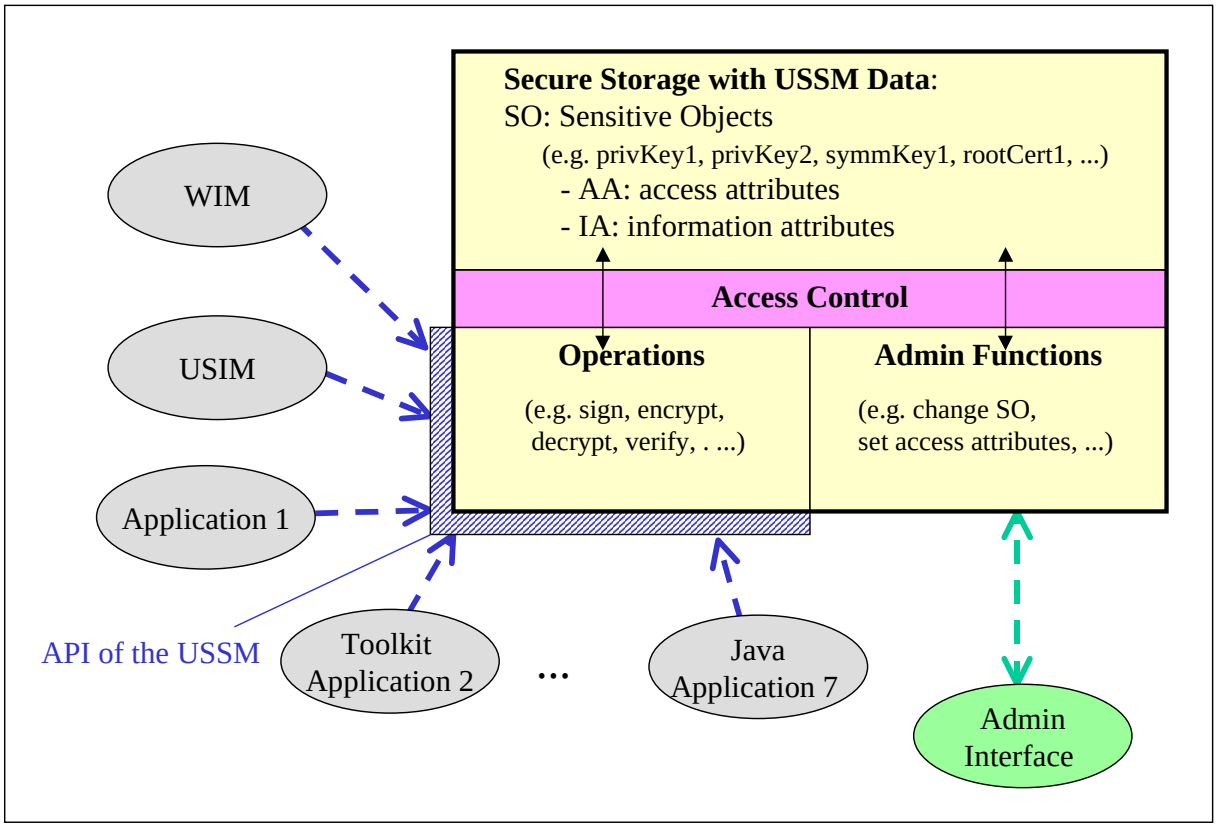



**Figure 1: Logical components of the USSM**

The USSM consists of the following logical components:

a) Secure storage, which contains sensitive objects and their access and information attributes.

b) Administrative functions, which are used to administer the USSM.

c) Operations, which are usable by card applications and can be accessed via an API.

d) Access control, which checks that access conditions are met.

The USSM contains the following type of data:

a) Sensitive data: Although it is recognized that probably all objects of the USSM are sensitive, for the purpose of the present document the term "Sensitive Object (SO)" is used for the keys and pins etc.

b) Access attributes: For each SO there is some associated access information to control the use of the SO. These Access Attributes (AA) contain the conditions that must be fulfilled before an operation can be performed using a sensitive object. Through AAs it is possible to limit the access to a SO to specific applications, to specific operations and to define which authentication must have been fulfilled.

c) Information attributes: For each SO there may be some associated information which describe the SO. This information may be read by a card application through the API.

# 5 Functional Requirements

## 5.1 USSM Admin Functions

USSM objects need to be securely administered. This shall be possible through USSM Admin Functions. The administration shall not be limited to personalization, but shall also be possible in the field, e.g. via OTA.

End-to-end security may be required between the USSM Administrator and the USSM, which is independent of OTA transport security. This end-to-end security shall provide:

- confidentiality of sensitive data,
- integrity of the command data,
- authentication of the sender,
- protection against replay, and
- proof of execution.

It shall be possible to configure the USSM to require none, some or all of these security features.

It shall be possible to have several USSMs on a card, each storing its own SOs, IAs and AAs. Each USSM is administered by its owner. Initial keys for secure administration may be loaded at point of manufacturing.

It is up to the card issuer policy to decide on the number of USSMs, the available memory per USSM, delegated management, etc.

The following figure shows an example with several USSMs in a card and the interaction between applications and USSMs.

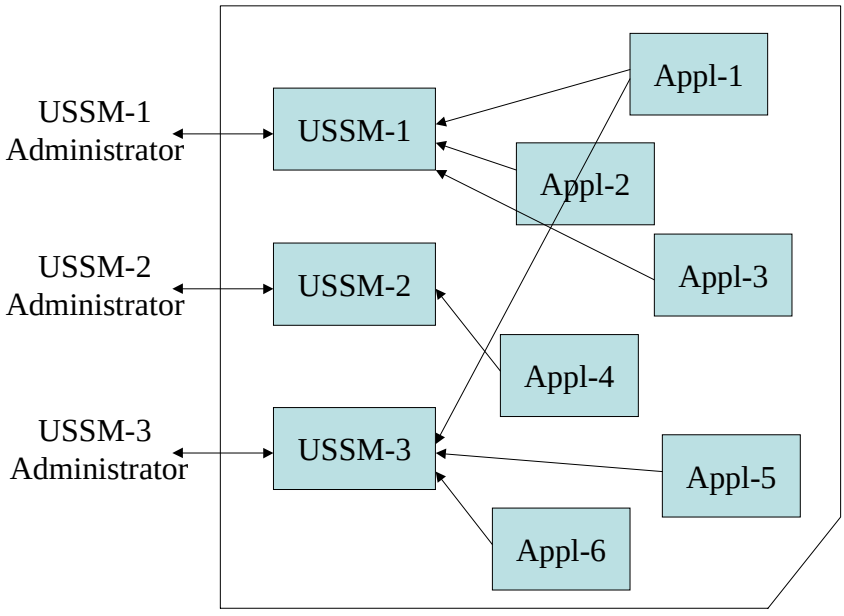



**Figure 2: Example with several USSMs**

The following table summarizes management functions that shall be defined in the first version of the stage 2 document. Depending on the implementation some USSMs may not support all of the following management functions.

**Table 1: List of Admin Functions**

| Function | Comment |
|---|---|
| Management of Sensitive Objects | - add (create) / update / erase a SO on the USSM<br>- retrieve / set / change attributes of a SO<br>- read a "readable" SO (e.g. a public key, root-certificate, certificate URL)<br>- link SOs together, e.g. a private key on the USSM to corresponding user certificates/URLs<br>- secure deletion of SO (e.g. overwrite with 0xFF)<br>- switch between two states 'inactive' and 'active'. Inactive SOs cannot be used by USSM operations.<br>- terminate an SO (i.e. the identifier of the SO is kept on the card, but the SO is no longer usable)<br>- mark an SO as security critical. It will automatically be terminated and its sensitive data be securely deleted if the associated authentication object (e.g. PIN) is blocked. |
| Management functions related to authentication | - set / change the value of a PIN, even when blocked (i.e. free blocked PIN)<br>- block/unblock authentication objects<br>- set retry counters<br>- link a SO to an authentication object |
| Key generation | - trigger generation of new RSA key pair within the USSM |
| Management of USSM | - read/update/delete information about the USSM<br>- retrieve remaining memory of USSM |

Objects are administered by the USSM owner, even a private key. However a private key with a non-repudiation flag is never readable/extractable by the USSM owner (although it might be deletable).

The concept of the USSM shall be flexible enough to allow the addition of new management functions in future versions of the specification.

## 5.2 Sensitive Objects and Operations

This clause defines sensitive objects and standardized operations that can be used with these objects. These operations can be used by applications on the UICC via an API.

The framework of the USSM shall be flexible enough to allow the addition of other types of sensitive data and other operations.

The following types of sensitive objects shall be defined in the first version of the stage 2 specification. Depending on the implementation some USSMs may not support all of the following objects.

- Private RSA keys
- Public RSA keys
- PINs
- Symmetric keys
- Root certificates
- User certificates
- Certificate URLs

The following table summarizes operations which shall be supported by the USSM if the corresponding types of sensitive data objects are supported. The exact definition of the supported operations in the first version of the USSM (e.g. RSA encryption according to RSAES PKCS v1_5 ENCRYPT [2]) will be specified in the stage 2 document.

These operations can be used with (shareable) SOs available in the USSM according to their type and access attributes.

**Table 2: List of operations**

| Operations | Comment |
|---|---|
| Verification operations | - read information which authentication rules are associated to a SO<br>- perform the authentication required for using a SO. At least the following two methods shall be supported:<br>* Verification of a PIN held within the USSM<br>* Authentication using a response to a challenge generated by the USSM |
| Asymmetric key operations | - signature generation<br>- signature verification<br>- decryption<br>- encryption |
| Symmetric key operations | - signature generation<br>- signature verification<br>- decryption<br>- encryption |
| Information functions | - Read an attribute of a SO<br>- read attributes of a USSM (e.g. owner, supported features, manufacturer, ...)<br>- read a public key, certificate URL, certificate |
| Export operations | - Export a selfsigned certificate request of a private key |

Note that the USSM will not allow every operation with every SO: Operations that are possible on an SO are limited by the type of the SO (e.g. an RSA key can not be used for DES operations) and the usage attributes assigned to it (e.g. a sign only key can not be used for decryption).

In addition further access restrictions specific to applications as defined in the next section may apply.

## 5.3 Restricted Access

Each sensitive object in the USSM has access attributes, which contain information on conditions that must be fulfilled before the SO can be used.

It must be possible to restrict the use of an SO to combinations of:

- specific applications;
- a specific subset of the operations allowed for the SO;
- verification conditions that must be fulfilled (e.g. a PIN to be verified).

Each time an application requests an operation with a specific SO, the USSM must check if the application is allowed to use this specific operation with this specific SO. The USSM must guarantee that the access conditions are met before the operation with the SO can be executed.

## 5.4 Information Attributes

For each SO in the USSM there may be information attributes. Applications may read these attributes.

Readable information attributes may be:

- A label, e.g. "OP-Transport-key";
- usage flags;
- Other attributes, e.g. if the SO was created outside or within the USSM, a key length.

# Annex A (informative): Notes

The following notes are informative and are intended to help understanding the USSM concept.

- Each application may keep it's own information of a SO which is known to this application. A WIM [3]for example can keep it's CDF, PrKDF etc. in it's own application-DF; the pointers however may point into the USSM, i.e. a private key itself is in the USSM and may also be used by other applications).
- Note that it is not mandatory to store every SO in the USSM. An application can keep it's own objects (which are not shared with other applications) in it's own memory. However it is possible that the USSM stores all relevant data that is shared between several applications, to save memory in the UICC.
- By sharing keys it is possible to use the same private key for signing operations by both a WIM and e.g. a card resident application.
- It is also possible that a terminal uses the USSM. One possible solution is to standardize an application on the UICC which understands and "translates" the APDUs sent by the terminal. This application acts as a "proxy" for the terminal.

# Annex B (informative): Change history

This annex lists all change requests approved for the present document since the first version was approved.

| Meeting | Plenary Tdoc | WG tdoc | VERS | CR | REV | CAT | SUBJECT | Resulting Version |
|---|---|---|---|---|---|---|---|---|
| SCP-20 | SCP-050068 | | 2.0.1 | | | | Publication | 7.0.0 |
| SCP:-23 | SCP-050474 | | 7.0.0 | 001 | - | D | | 7.1.0 |

# History

| Document history | | |
|---|---|---|
| V7.0.0 | June 2005 | Publication |
| V7.1.0 | January 2006 | Publication |
| | | |
| | | |
| | | |