(U)SIM Java Card Platform Protection Profile

Basic and SCWS Configurations

Evolutive Certification Scheme for (U)SIM cards

Emission Date	:	June 17th, 2010
Reference	:	PU-2009-RT-79
Version	:	2.0.2
Classification	:	Public
Number of Pages	:	85 (including 2 header pages)

SFR

AFOM
ASSOCIATION FRANÇAISE
DES OPÉRATEURS MOBILES

Trusted Labs

DISCLAIMER OF WARRANTY

This Document is provided "as is" and all express or implied conditions, representations and warranties, including, but not limited to, any implied warranty of merchantability, fitness for a particular purpose or non-infringement, are disclaimed, except to the extent that such disclaimers are held to be legally invalid. SFR S.A., Trusted Labs S.A.S and Association Française des Opérateurs Mobiles (AFOM) shall not be liable for any special, incidental, indirect or consequential damages of any kind, arising out of or in connection with the use of this Document.

COPYRIGHT NOTICE

Contact

For SFR:

Maryline Eznack: maryline.eznack@sfr.com
Jean Philippe Wary: jean-philippe.wary@sfr.com

For Trusted Labs:

Claire Loiseaux: claire.loiseaux@trusted-labs.com
Guillaume Dufay: guillaume.dufay@trusted-labs.com
Roland Atoui: roland.atoui@trusted-labs.com

For AFOM:

Nicolas Herbreteau: nherbreteau@afomobiles.org
Jakub Pieniazek: jpieniaz@bouyguestelecom.fr
Frédéric Thabaret: frederic.thabaret@orange-ftgroup.com

We would like to specially thank the AEPM and EPOMI associations for their comments to the work done.

Table of Contents

List of Figures

List of Tables

1 Protection Profile Introduction

This Protection Profile (PP) is the foundation for the Evolutionary (U)SIM Java Card TM platforms Composition Scheme. As a unique combination of Common Criteria scheme and mobile operator Validation Scheme, it creates the necessary conditions of trust for delivering new types of applications for the mobile environment. Security demanding applications such as payment applications, mobile-TV applications, identity applications (hereafter referenced as Secure Applications) are now loaded onto EAL4+ certified smart cards embedding (U)SIM Java Card Platforms along with validated applications requiring less security (hereafter Basic applications) and this during the post-issuance of the Java Card TM platforms.

This advance opens the door for new usage models of Mobile Network Operators (MNOs) (U)SIM cards, compatible with increasing security demand. With help of the Common Criteria standard, it delivers for the first time in the mobile ecosystem, tangible benefits for all value-chain actors, including end-users.

In the following, the (U)SIM Java Card platform will called (U)SIM platform for short and the smart card product embedding the (U)SIM platform will be call (U)SIM card.

1.1.1 At the Edge of New Mobile Services

This Protection Profile takes place in the context of the explosion of services provided by MNOs which intend to open (U)SIM card to new applications.

In order to ensure end users and application providers trust, mandatory to guarantee the success of these new services, the evolutionary certification scheme is built in accordance with the industrial and market constraints. This work starts by defining the security rules required for such an open (U)SIM Java Card platform.

This is the goal of the present Protection Profile.

1.2 Protection Profile Identification

This document holds two Protection Profiles as indicated in the following tables.

Title:	(U)SIM Java Card TM Platform Protection Profile — Basic Configuration
Author:	Trusted Labs S.A.S.
Version:	June 17th, 2010, PP version 2.0.2
Sponsors:	Société Française du Radiotéléphone (SFR)
CC Version:	3.1 revision 3

Title:	(U)SIM Java Card TM Platform Protection Profile — SCWS Configuration
Author:	Trusted Labs S.A.S.
Version:	June 17th, 2010, PP version 2.0.2
Sponsors:	Société Française du Radiotéléphone (SFR)
CC Version:	3.1 revision 3

In the following, “this Protection Profile” stands for the Protection Profile collection composed of PP with Basic Configuration and with SCWS Configuration.

1.3 TOE Overview

This section presents the architecture and common usages of the Target of Evaluation (TOE).

The TOE of this Protection Profile is the (U)SIM Java Card platform of (U)SIM cards. This Protection Profile defines two TOE configurations, Basic and SCWS. Each TOE configuration gives rise to a Protection Profile configuration, with unique identification:

- “Basic Configuration” addresses products without the Smart Card Web Server (SCWS) functionality.
- “SCWS Configuration” addresses products with the SCWS functionality.

This Protection Profile focuses on the security requirements for the (U)SIM Java Card platform; the Smart Card Platform (SCP, the combination of the IC and the OS) is considered as the environment of the (U)SIM Java Card platform, covered by security objectives. Nevertheless, any (U)SIM smart card evaluation against this PP shall comprehend the whole including both the smart card platform and the (U)SIM platform as well as any pre-loaded applet.

1.3.1 TOE Type

The Target of Evaluation (TOE) is the (U)SIM Java Card platform embedded in a (U)SIM card intended to be plugged in a mobile phone or other mobile devices to provide services to an end user.

The Basic TOE is composed of the following bricks:

- A Java Card System according to [PP-JCS] which manages and executes applications called applets. It also provides APIs [JCAPI] to develop applets on top of it, in accordance with Java Card TM specifications.
- GlobalPlatform (GP) packages, which provides a common and widely used interface to communicate with a smart card and manage applications in a secure way, in accordance with [GP] specifications,
- (U)SIM APIs, which provides ways to specifically interact with (U)SIM applications, according to [TS131.130] specifications.

The SCWS TOE adds the following brick to the Basic TOE:

- Smart Card Web Server (SCWS) functionality, in accordance with [SCWS] specifications.

1.3.2 Basic TOE

The generic architecture of the Basic TOE is described hereafter (see Figure 1) and detailed in the following paragraphs. The non-TOE elements are described in Section 1.3.8.

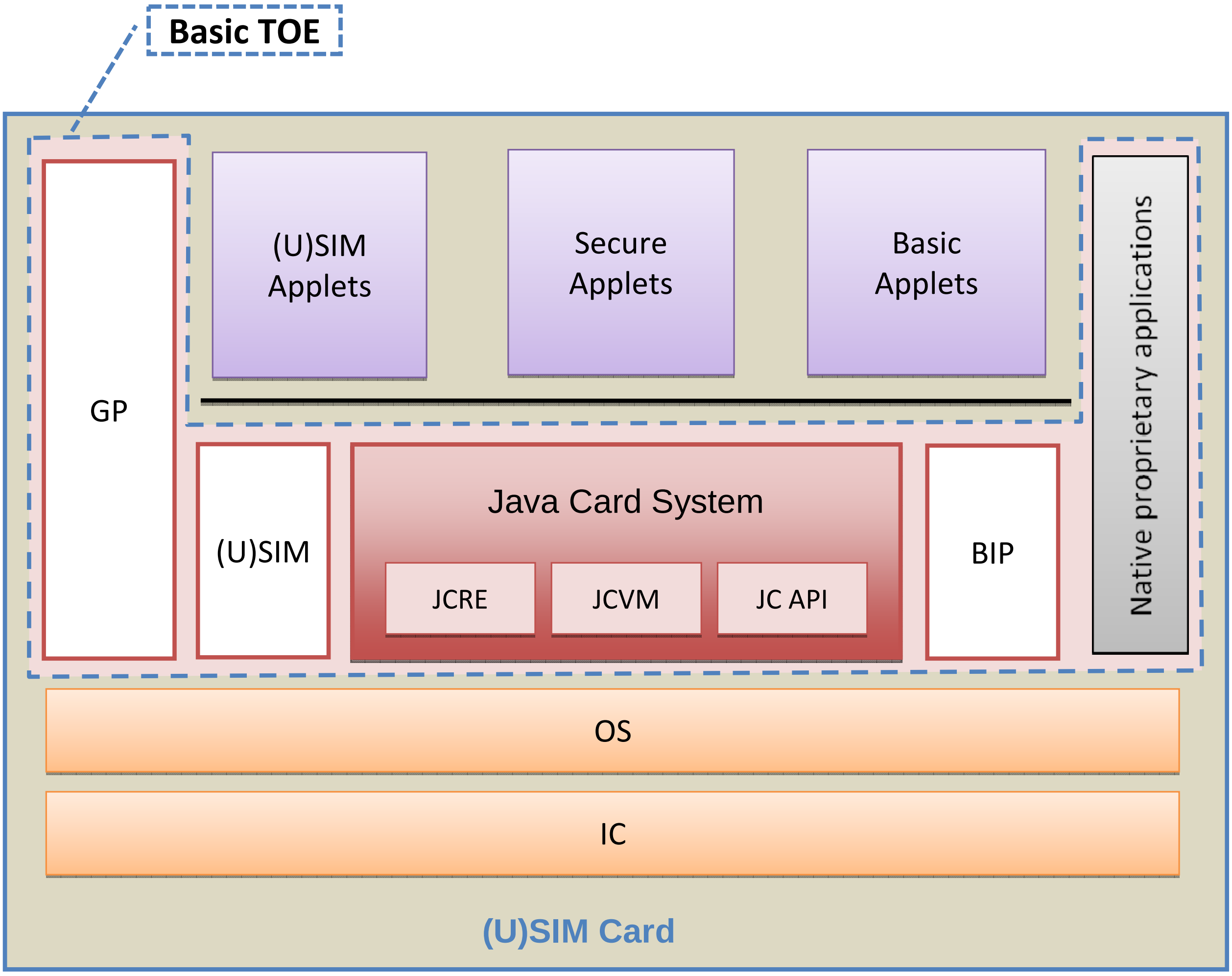

Figure 1: Open (U)SIM Java Card Platform architecture (Basic TOE)

1.3.2.1 (U)SIM Functionality

The (U)SIM specifications considered in this document is the Release 6 version of the ETSI 3GPP specification.

Data exchange between the TOE and the mobile network, including applications downloading are enforced through a communication channel based on SMS or BIP technology.

The (U)SIM supports at least the following APIs:

- The UICC API [TS102.241] is an extension of the SIM API [TS03.19] which provides the means for the applications to access the smart card file system, to subscribe in order to receive the events of the common application toolkit framework, to handle information received and to send proactive commands.
- The (U)SIM API [TS131.130] extends the UICC API to provide features related to the 3G: it provides the means for applets to get access to the files of the (U)SIM, to register to the events defined in the USAT specification, etc.

Any additional (U)SIM functionality should remain in the TOE.

1.3.2.2 Bearer Independent Protocol (BIP)

The BIP technology is an Over-The-Air (OTA) technology to exchange data between a (U)SIM card on a mobile phone and remote servers. It will replace the SMS technology as a data bearer for mobile phones.

The BIP technology relies on high speed communication protocols such as GPRS, EDGE, UMTS, Bluetooth, USB 2.0 and infrared of new generation mobile phones (2.5G and 3G). Therefore, the communication is faster and more reliable than through the SMS channel. Local communication channels with the SIM (Bluetooth, USB, infrared) are not supported in this protection profile.

This technology is a part of the TOE. It is specified in 3GPP specifications. In particular, [TS102.223], [TS102.225] and [TS131.111] are implemented.

The BIP technology does not offer any security function.

1.3.2.3 Java Card Platform

The Java technology, embedded on the TOE, combines a subset of the Java programming language with a runtime environment optimized for smart cards and similar small-memory embedded devices [JCVM]. The Java Card ^{TM} platform is a smart card platform enabled with Java Card ^{TM} technology (also called, for short, a “Java Card”). This technology allows for multiple applications to run on a single card and provides facilities for secure interoperability of applications. Applications running on the Java Card platform (“Java Card applications”) are called applets.

The TOE is compliant with the version of the Java Card platform specified in [JCVM], [JCRE] and [JCAPI]. It includes the Java Card Virtual Machine (Java Card VM), the Java Card Runtime Environment (Java Card RE) and the Java Card Application Programming Interface (Java Card API), detailed in the next paragraph. As the terminology is sometimes confusing, the term “Java Card System” has been introduced in [PP-JCS] to designate the set made of the Java Card RE, the Java Card VM and the Java Card API. The Java Card System provides an intermediate layer between the operating system of the card and the applications. This layer allows applications written for one smart card platform enabled with Java Card technology to run on any other such platform.

The Java Card VM is a bytecode interpreter embedded in the smart card. The Java Card RE is responsible for card resource management, communication, applet execution, on-card system and applet security.

The TOE is configured so that an applet can be downloaded and installed on it, even after the smart card has been issued to the Cardholder. This allows MNOs as Card issuers to dynamically respond to customers needs. For instance, if the Card issuer decides to upgrade some of the applications offered to the customer, this could be made without issuing a new card. Moreover, applications from different vendors can coexist in a single card, and they can even share information between each other. Since a smart card application is usually intended to store highly sensitive information, the sharing of that information must be carefully controlled.

Applet isolation is achieved through the Java Card Firewall mechanism defined in [JCRE]. That mechanism confines an applet to its own designated memory area. Thus, each applet is prevented from accessing fields and operations related to objects owned by other applets, unless those applets provide a specific interface (shareable interface) for that purpose. This access control policy is enforced at runtime by the Java Card VM.

However, applet isolation cannot be entirely granted by the firewall mechanism if certain well-formedness conditions are not satisfied by loaded applications. Therefore, a bytecode verifier (BCV) formally verifies those conditions. The BCV is out of the scope of the Java Card System defined in [PP-JCS].

This Protection Profile addresses versions 2.2.x and 3.0.x Classic Edition of the Java Card platform specifications.

The Java Card API (JCAPI) provides classes and interfaces for the core functionality of a Java Card application. It defines the calling conventions by which an applet may access the JCRE and services such as, among others, I/O management functions, PIN and cryptographic specific management and the exceptions mechanism. The JCAPI is compatible with formal international standards, such as ISO 7816 and industry specific standards (such as EMV, Calypso).

1.3.2.4 GlobalPlatform

The TOE is compliant with the GlobalPlatform (GP) standard [GP] which provides a set of APIs and technologies to perform in a secure way, the operations involved in the management of the applications hosted by the card. Using GP maximizes the compatibility and the opportunities of communication as it becomes the current card management standard.

The main features addressed by GP are:

- the authentication of users through secure channels,
- the downloading, installation, removal, and selection for execution of Java Card applications,
- the life-cycle management of both the card and the application,
- the sharing of a global common PIN among all the applications installed on the card.

These operations are addressed by a set of APIs used by the applications hosted on the card in order to communicate with the external world on a standard basis.

The version considered in this document is GP version 2.2 of the specification. The following GP functionalities, at least, are present within the TOE:

- Card content loading
- Extradition
- Asymmetric keys
- DAP support
- Mandated DAP support
- DAP calculation with asymmetric cryptography
- Logical channels
- SCP02 support
- SCP80 support defined by the ETSI [TS102.225] (mandatory for the ISD)

- Support for contactless cards (ATQ, different implicit selection on different interfaces and channels)
- Support for Supplementary Security Domains
- Installation of Security Domains
- Trusted Path privilege
- Delegated Management privilege
- Post-issuance personalization of Security Domain [GP-UICC]
- Application personalization [GP-UICC]

The Authorized Management privilege is not supported by this Protection Profile.

1.3.3 SCWS TOE

The generic architecture of the SCWS TOE is described hereafter (see Figure 2). It extends the Basic TOE (see Section 1.3.2) with the SCWS functionality detailed in the following paragraph. The non-TOE elements are described in Section 1.3.8.

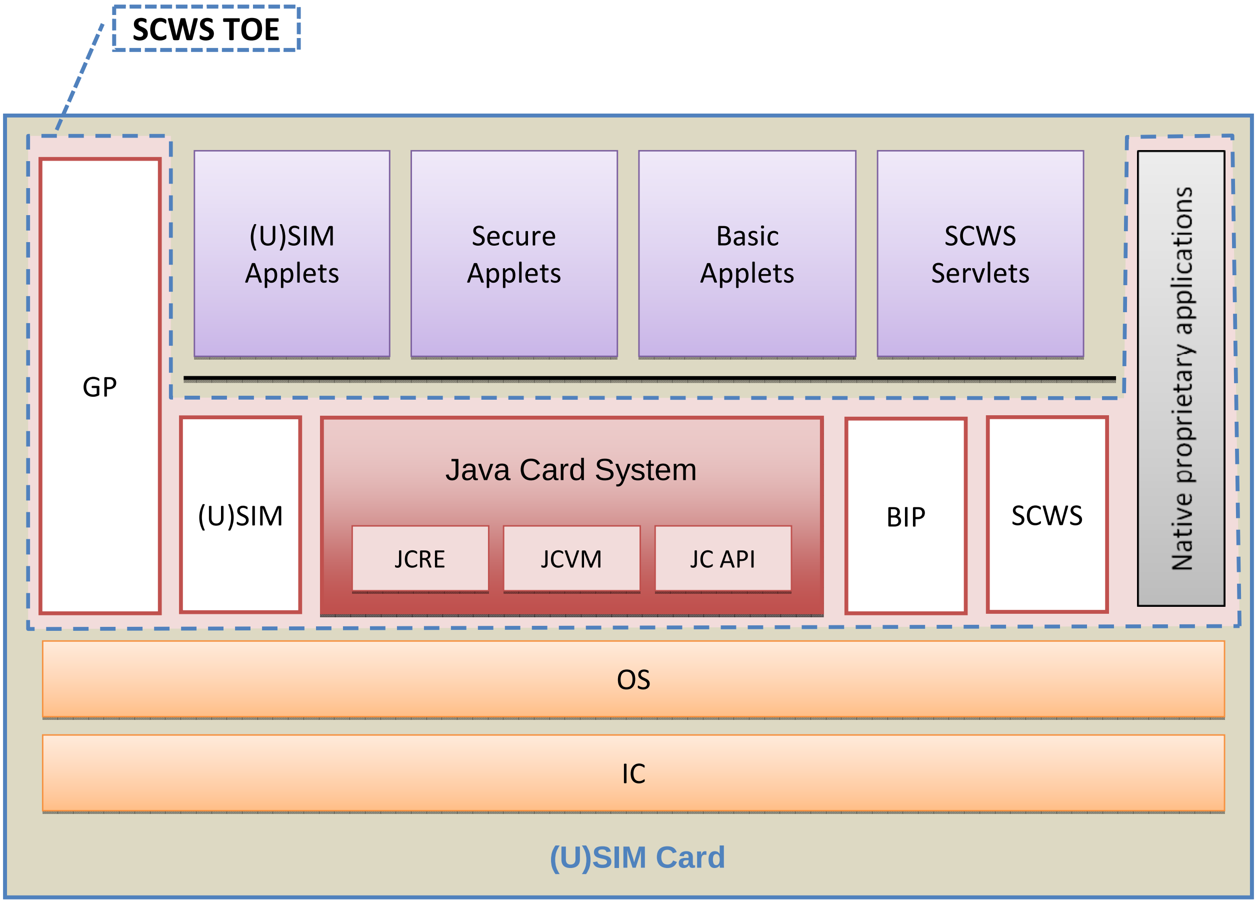

Figure 2: Open (U)SIM Java Card^{TM} Platform architecture (SCWS TOE)

1.3.3.1 Smart Card Web Server (SCWS)

The SCWS technology [SCWS] brings a HTTP Web Server on the (U)SIM card, enabling the end-user to access the (U)SIM contents and applications through a familiar and standardized interface, the web browser of its mobile phone. New services and configuration options can then be brought to the end-user.

The SCWS specifications cover:

- the local communications between a web browser running on the mobile phone and the SCWS application on the (U)SIM, through a SCWS gateway in the mobile
- the behaviour of the SCWS application on HTTP(S) requests
- the interactions between the SCWS application and SCWS-based services
- the remote administration of the SCWS by authorized entities (Card Issuer, MNO or Application Provider) which includes modification of static web pages and registration of installed servlets to the SCWS server

On the (U)SIM card, the SCWS architecture relies on:

- the SCWS application which manages the HTTP requests and provides registering mechanisms to applets
- an API package that provides methods for applets to register to the SCWS server so as to receive HTTP requests and send responses
- a runtime environment SCWS (SCWS RE) that enables the communication between the SCWS server and the applets
- a package of applets providing SCWS servlets

1.3.4 TOE Usage

The SIM, defined in the 3GPP standards as the Subscriber Identity Module, is a removable module within GSM mobile equipment that contains the International Mobile Subscriber Identity (IMSI) which unambiguously identifies a subscriber. When the SIM is placed in a mobile equipment, users can register onto the GSM network. The primary function of the SIM is consequently used to authenticate the validity of a terminal when accessing the network. It also provides a means to authenticate the end user and may store other subscriber-related information or applications such as SIM Toolkit applications as specified in [TS102.223] and [TS131.111].

The SIM is the MNO's property, and stores MNO's specific information. The USIM defined in the 3GPP standards as the Universal Subscriber Identity Module is an evolution of the SIM developed to ensure compliance within UMTS networks (also called 3G). This new generation of SIM especially includes improvements of mutual authentication mechanisms.

Note:

In the following SIM and USIM are considered in the same way regarding security. This is why the term of (U)SIM is used to refer to SIM or USIM. This Protection Profile addresses the case of (U)SIM cards with embedded Java Card platforms.

1.3.5 TOE Life Cycle

The TOE life cycle follows the description of the [PP-JCS] and is part of the product life cycle, i.e. the (U)SIM card, which goes from product development to its usage by the final user.

The product life cycle phases are those detailed in Figure 3. We refer to [PP0035] for a thorough description of Phases 1 to 7:

- Phases 1 and 2 compose the product development: Embedded Software (IC Dedicated Software, OS, Java Card System, (U)SIM applet, other platform components such as Card Manager, Applets) and IC development.
- Phase 3 and 4 correspond to IC manufacturing and packaging, respectively. Some IC pre-personalisation steps may occur in Phase 3.
- Phase 5 concerns the embedding of software components within the IC.
- Phase 6 is dedicated to the product personalisation prior final use.
- Phase 7 is the product operational phase.

The (U)SIM platform life cycle is composed of four stages:

- Development,
- Storage, pre-personalisation and test,
- Personalization and test,
- Final usage.

(U)SIM platform storage is not necessarily a single step in the life cycle since it can be stored in parts. (U)SIM platform delivery occurs before storage and may take place more than once if the TOE is delivered in parts. These stages map to the typical smart card life cycle phases as shown in Figure 3.

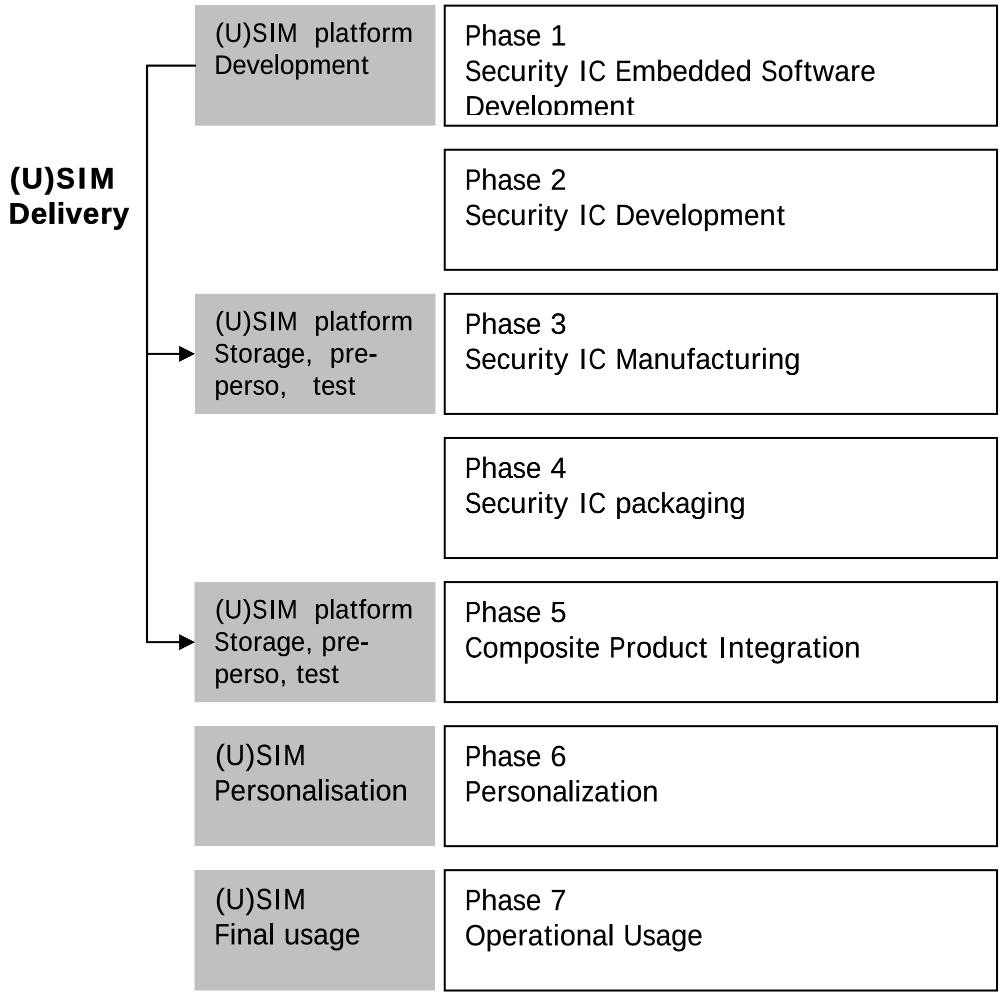
(U)SIM Delivery
(U)SIM platform Development
Phase 1
Security IC Embedded Software Development
Phase 2
Security IC Development
(U)SIM platform Storage, pre-perso, test
Phase 3
Security IC Manufacturing
Phase 4
Security IC packaging
(U)SIM platform Storage, pre-perso, test
Phase 5
Composite Product Integration
(U)SIM Personalisation
Phase 6
Personalization
(U)SIM Final usage
Phase 7
Operational Usage

Figure 3: (U)SIM platform (TOE) Life Cycle within Product Life Cycle

(U)SIM platform Development is performed during Phase 1. This includes Java Card System (JCS) and (U)SIM conception, design, implementation, testing and documentation. The development shall fulfil requirements of the final product, including conformance to Java Card Specifications, and recommendations of the SCP user guidance. The development shall occur in a controlled environment that avoids disclosure of source code, data and any critical documentation and that guarantees the integrity of these elements. The evaluation of a product against this PP shall include the (U)SIM platform development environment.

The delivery of the (U)SIM platform may occur either during Security IC Manufacturing (Phase 3) or during Composite Product Integration (Phase 5). It is also possible that part of the (U)SIM platform is delivered in Phase 3 and the rest is delivered in Phase 5. Delivery and acceptance procedures shall guarantee the authenticity, the confidentiality and integrity of the exchanged pieces. (U)SIM platform delivery shall usually involve encrypted signed sending and it supposes the previous exchange of public keys. The evaluation of a product against this PP shall include the delivery process.

In Phase 3, the Security IC Manufacturer may store, pre-personalize the (U)SIM platform and potentially conduct tests on behalf of the developer. The Security IC Manufacturing environment shall protect the integrity and confidentiality of the (U)SIM platform and of any related material, for instance test suites. The evaluation of a product against this PP shall include the whole Security IC Manufacturing environment, in particular those locations where the (U)SIM platform is accessible for installation or testing. If the Security IC has already been certified (e.g. against [PP0035]) there is no need to perform the evaluation again.

In Phase 5, the Composite Product Integrator may store, pre-personalize the (U)SIM platform and potentially conduct tests on behalf of the developer. The Composite Product Integration environment shall protect the integrity and confidentiality of the (U)SIM platform and of any related material, for instance test suites. Note that (part of) (U)SIM platform storage in Phase 5 implies a product delivery after Phase 5. Hence, the evaluation of such product against this PP shall include the Composite Product Integrator environment (may be more than one if there are many integrators).

The (U)SIM platform is personalized in Phase 6, if necessary. The Personalization environment shall be included in a product evaluation only if the product delivery point is at the end of Phase 6. This means that some of the product personalization operations may require a controlled environment (secure locations, secure procedures and trusted personnel). The product shall be tested again and all critical material including personalization data, test suites and documentation shall be protected from disclosure and modification. During this phase, MNO (ISD keys and other initial data), Certification Authority and Verification Authority data are loaded on the (U)SIM. After this phase, the (U)SIM card reaches its INITIALIZED state.

The (U)SIM platform final usage environment is that of the product where the (U)SIM platform is embedded in. It covers a wide spectrum of situations that cannot be covered by evaluations. The (U)SIM platform and the product shall provide the full set of security functionalities to avoid abuse of the product by untrusted entities.

Card management (including Secure or Basic applications loading and personalization) can occur during production in a secure area in phase 5 or 6 or during the product usage in phase 7 using an OTA bearer.

Application note: *The Security Target writer shall specify the life cycle of the product, the (U)SIM platform delivery point and the product delivery point. The product delivery point may arise at the end of Phase 3, 4, 5 or 6 depending on the product itself. Note that (U)SIM platform delivery precedes product delivery. During product evaluation against this Protection Profile, the ALC security assurance requirements apply to the whole product life cycle up to delivery.*

1.3.6 Actors of the TOE

One of the characteristics of the (U)SIM Java Card platforms is that several entities are represented inside these platforms:

- The **Mobile Network Operator** (MNO or mobile operator), issuer of the (U)SIM Java Card platform and proprietary of the TOE. The TOE guarantees that the issuer, once authenticated, can manage the loading, instantiation and deletion of applications.
- The **Application Provider** (AP), entity or institution responsible for the applications and their associated services. It is a financial institution (a bank), a transport operator or a third party operator.
- The **Controlling Authority** (CA), entity independent from the MNO represented on the (U)SIM card and responsible for securing the keys creation and

personalization of the Application Provider Security Domain (APSD) (Push and Pull personalization model of [GP-UICC]).

- The **Verification Authority** (VA), trusted third party represented on the (U)SIM card, acting on behalf of the MNO and responsible for the verification of applications signatures (mandated DAP) during the loading process. These applications shall be validated for the Basic ones or certified for the secure ones.

1.3.7 TOE Security Features

Secure or Basic applets can be loaded and instantiated onto the TOE either before card issuance or over-the-air (OTA) in post-issuance through the mobile network, without physical manipulation of the TOE and in a connected environment. Besides these, other administrative operations can also be done OTA.

The main security feature of the TOE is the correct and secure execution of sensitive applications, in a connected environment and with the presence on the TOE of Basic (non-certified) applications.

1.3.7.1 Security Services to Applications

The TOE offers to applications a panel of security services in order to protect application data and assets:

- Confidentiality and integrity of cryptographic keys and associated operations. Cryptographic operations are protected, including protection against observation or perturbation attacks. Confidentiality and integrity of cryptographic keys and application data are guaranteed at all time during execution of cryptographic operations.
- Confidentiality and integrity of authentication data. Authentication data are protected, including protection against observation or perturbation attacks. Confidentiality and integrity of authentication data and application data are guaranteed at all time during execution of authentication operations.
- Confidentiality and integrity of application data among applications. Applications belonging to different contexts are isolated from each other. Application data are not accessible by a normal or abnormal execution of another Basic or Secure application.
- Application code execution integrity. The Java Card VM and the “applications isolation” property guarantee that the application code is operating as specified in absence of perturbations. In case of perturbation, this TOE security feature must also be valid.

1.3.7.2 Application Management

The TOE offers additional security services for applications management, relying on the GlobalPlatform framework:

- The MNO as Card issuer is initially the only entity authorized to manage applications (loading, instantiation, deletion) through a secure communication channel with the card, based on SMS or BIP technology. However, the MNO can grant these privileges to the AP through the delegated management functionality of GP.

- Before loading, all applications are verified by a validation laboratory for the Basic applications, or by an ITSEF for the secure applications. All loaded applications are associated at load time to a Verification Authority (VA) signature (Mandated DAP) that is verified on card by the on-card representative of the VA prior to the completion of the application loading operation and prior to the instantiation of any applet defined in the loaded application.
- Application Providers personalize their applications and Security Domains (APSD) in a confidential manner. Application Providers have Security Domain keysets enabling them to be authenticated to the corresponding Security Domain and to establish a trusted channel between the TOE and an external trusted device. These Security Domains keysets are not known by the Card issuer.

Basic and Secure applets (as defined below) are loaded in different Java Card packages.

1.3.8 Non-TOE HW/SW/FW Available to the TOE

1.3.8.1 Integrated Circuit (IC) or Chip

The TOE is based on a Security IC which is a hardware device composed of a processing unit, memories, security components and I/O interfaces. It has to implement security features able to ensure:

- The confidentiality and the integrity of information processed and flowing through the device,
- The resistance of the Security IC to externals attacks such as physical tampering, environmental stress or any other attacks that could compromise the sensitive assets stored or flowing through it.

This Security IC may also include:

- Extra features such as SWP interface.
- Embedded proprietary software called IC Dedicated Software (or firmware) which provides additional services (such as low level routines) to facilitate the usage of the Security IC.

1.3.8.2 Operating System (OS)

The TOE relies on an Operating System (OS) which is an embedded piece of software loaded into the Security IC and which manages the features and resources provided by the underneath chip. It is, generally divided into two levels:

1) Low level:
    - Drivers related to the I/O, RAM, ROM, EEPROM, Flash memory if any, and any other hardware component present on the Security IC,
2) High Level:
    - Protocols and handlers to manage I/O,
    - Memory and file manager,
    - Cryptographic services and any other high level services provided by the OS.

1.3.8.3 Mobile Terminals

The (U)SIM as a smartcard is intended to be plugged in a mobile handset. This equipment can be a mobile phone or a PDA or any other connecting device.

It must be stressed out that for applets requiring user interaction, such as PIN entry, devices that interact with the TOE must be trusted and follow security rules. These rules can range from security audits to CC certification and depend from the operational environment expected from the applet.

1.3.8.4 Basic Applets

Basic applets stand for applications that do not require any particular security for their own. This is the case for fidelity applications, Information-on-demand (IOD) applications, etc.

Basic applications must be compliant with the security rules of the TOE. This compliance is analyzed through a validation process by a validation laboratory ensuring that the recommendations and restrictions of the (U)SIM certification report are still valid (the conditions of the product usage are compliant with the Certification report). Once validated, these applications are signed by the VA. The MNO as Card issuer then authorizes the Basic applications loading onto the TOE. The application signature is verified by a representative of the VA on card prior to any application loading or instantiation.

For the SCWS TOE, a SCWS servlet is a Standard Java Card applet registered to the SCWS and mapped on one or several URIs. It provides dynamic content to the SCWS.

1.3.8.5 Secure Applets

Secure applets are applications requiring a high level of security for their own assets. It is indeed necessary to protect application assets in confidentiality, integrity or availability at different security levels depending on the AP Security Policy. This is typically the case for payment applications, requiring a high level of security assurance (the Common Criteria EAL4 with AVA_VAN.5 or higher EAL is required), for conditional access mobile TV applications or digital signature applications (in Europe, the PP [SSCD] is required for qualified digital signature applications).

As such, secure applications follow a Common Criteria evaluation and certification in composition with the previously certified (U)SIM smart card [Secure APP].

1.3.8.6 Terminals, Remote Servers and Trusted IT Products

Using its NFC (contactless) interface, the TOE can communicate with a card reader such as POS (Point of Sale) equipments or ticketing systems terminals. These terminals are responsible for the protection of their own assets.

Using the BIP interface or SMS, the TOE can also communicate with remote servers, for instance for remote administration or transfer of applicative data. For sensitive operations, such as remote administration, the TOE may require mutual authentication or the use of secure channels. In that case, the keys and/or certificates required for these operations on the TOE will also have to be available from the remote server and protected. The remote server and, if any, the device (such a HSM) from which the keys are obtained are referred as a Trusted IT product.

1.3.9 Protection Profile Usage

The TOE of a Security Target conformant with this PP is the whole (U)SIM card made of the IC and all the embedded software, including the (U)SIM Java Card platform. The objectives for the environment (i.e. for the IC and the OS) specified in this PP shall become objectives for the TOE in the Security Target. These objectives shall be (1) either fulfilled by a previous certificate or (2) translated into SFRs by the ST author, or (3) a combination of both.

- The first scenario corresponds to a composite evaluation in the sense of [Comp], with the IC and the OS already certified, and the (U)SIM Java Card platform certified on top of them. The Security Target shall refer to the IC and OS Security Target(s) to fulfill the IC and OS security objectives.
- The second scenario corresponds to a unified evaluation of the whole product. The ST shall define SFRs for the IC and the OS in addition to those specified in this PP.
- The third scenario arises for instance when the (U)SIM Java Card Platform is embedded in a certified IC, but the OS features have not been certified. Therefore, the ST shall refer to the IC Security Target to fulfill the IC objectives and shall introduce SFRs in order to meet the objectives for the OS. This is a composite evaluation of the system composed of the (U)SIM Java Card platform and the OS on top of a certified IC.

The ST author is allowed to add objectives for the TOE regarding other aspects than those specified in this Protection Profile provided the CC conformance rules are met. This may arise, for instance, if the product includes a secure application with specific requirements (e.g. a signature application that must fulfill [PP-SSCD]). In particular, in a composite evaluation [Comp], a composite product Security Target (typically for a TOE composed of the (U)SIM Java Card platform with secure applications) will have to compose with several application security requirements:

- Where there is no application Protection Profile, the composite product Security Target describes the security requirements of the secure application embedded into the previously certified TOE.
- When an application Protection Profile has already been certified, the (U)SIM Java Card platform security requirements are described within the new composite product Security Target.

The (U)SIM Java Card platform being evaluated and certified at EAL4+ level, the secure application embedded into the (U)SIM Java Card platform is certified in composition [Comp] at a maximum assurance level of EAL4+.

For specific needs, some security functions of the secure application may envisage to pursue a higher security assurance level (typically using formal methods) for the secure application only and outside composition activities. The additional elements of evidence on the secure application reinforce the trust on the security level of the application.

2 Conformance Claims

2.1 CC Conformance Claims

This protection profile is conformant to Common Criteria version 3.1 revision 3. More precisely, this protection profile is:

- CC Part 1 [CC1],
- CC Part 2 conformant [CC2],
- CC Part 3 conformant [CC3],

The assurance requirement of this Protection Profile is **EAL4 augmented**. Augmentation results from the selection of:

- **ALC_DVS.2** Sufficiency of security measures.
- **AVA_VAN.5** Advanced methodical vulnerability analysis

2.2 PP Conformance Claims

This PP is conformant to the "Java Card System Open Configuration Protection Profile" [PP-JCS].

This Protection Profile does not require formal compliance to a specific IC Protection Profile or a smart card OS Protection Profile but those IC and OS evaluated against [PP0035] and [PP0902] respectively, fully meet the objectives.

2.3 Conformance Claims to this PP

This Protection Profile requires **demonstrable** conformance (as defined in [CC1]) of any ST or PP claiming conformance to this PP.

2.4 Conformance Claims Rationale

What follows reveals the consistency between this PP and the [PP-JCS] to which conformance is being claimed. [PP-JCS] requires demonstrable conformance.

2.4.1 TOE Type Conformance

The TOE type in the (U)SIM Java Card Platform comprehends the Java Card System defined in the TOE type of [PP-JCS], including all the native code. Hence TOE type consistency is achieved.

2.4.2 SPD Statement Consistency

The entire Java Card System threats, OSPs and assumptions are relevant to the TOE as defined in this PP.

In order to precisely state the relationship between assets, threats, OSPs or assumptions of Java Card System SPD and assets, threats, OSPs or assumptions of this PP SPD, three notions will be used:

- Equivalence: threats, OSPs or assumptions in this PP are the same than in [PP-JCS] but apply to additional assets defined in this PP.
- Refinement: this PP's assets, threats, OSPs or assumptions are more restrictive than the ones required in [PP-JCS] SPD.
- Addition: this PP specifies additional assets threats, OSPs or assumptions that are independent from [PP-JCS] SPD and do not affect it.

2.4.2.1 Assets

All assets of [PP-JCS] are included in this PP.

Assets from this PP	Conformance rationale with [PP-JCS]
D.APSD_KEYS	Refinement of D.APP_KEYS of [PP-JCS]
D.CASD_KEYS	Refinement of D.APP_KEYS of [PP-JCS]
D.ISD_KEYS	Refinement of D.APP_KEYS of [PP-JCS]
D.VASD_KEYS	Refinement of D.APP_KEYS of [PP-JCS]
D.GP_CODE	Addition to [PP-JCS]
D.CARD-MNGT-DATA	Addition to [PP-JCS]
D.(U)SIM-CODE	Refinement of D.JCS-CODE of [PP-JCS]
D.(U)SIM-DATA	Refinement of D.JCS-DATA of [PP-JCS]
D.SCWS-CODE	Addition to [PP-JCS] for SCWS
D.SCWS-AUTH	Addition to [PP-JCS] for SCWS
D.SCWS-DATA	Addition to [PP-JCS] for SCWS

2.4.2.2 Threats

All threats of [PP-JCS] are included in this PP.

Threats from this PP	Conformance rationale with [PP-JCS]
T.PHYSICAL	Equivalent to T.PHYSICAL of [PP-JCS]. Applies to the new assets introduced in the (U)SIM PP
T.INTEG-USER-DATA	Refinement of T.INTEG-APPLI-DATA of [PP-JCS]. Applies to (U)SIM PP assets
T.COM_EXPLOIT	Addition. Applies to (U)SIM communication channels
T.UNAUTHORIZED_CARD_MNGT	Refinement of T.INSTALL of [PP-JCS]
T.LIFE_CYCLE	Addition. Applies to card content management
T.UNAUTHORIZED_ACCESS	Refinement of T.CONFID-APPLI-DATA of [PP-JCS] to Shareable Objects
T.SCWS_FLAW	Addition to [PP-JCS] for SCWS
T.OBSOLETE_CONF	Addition to [PP-JCS] for SCWS
T.REPLAY	Addition to [PP-JCS] for SCWS
T.DOS	Addition to [PP-JCS] for SCWS

2.4.2.3 OSPs

All OSPs of [PP-JCS] are included in this PP.

Organisational Security Policies	Conformance rationale with [PP-JCS]
OSP.SECURE-APPS-CERTIFICATION	Refinement of OSP.VERIFICATION of [PP-JCS]
OSP.BASIC-APPS-VALIDATION	Refinement of OSP.VERIFICATION of [PP-JCS]
OSP.SHARE-CONTROL	Refinement of OSP.VERIFICATION of [PP-JCS]
OSP.AID-MANAGEMENT	Refinement of OSP.VERIFICATION of [PP-JCS]
OSP.OTA-LOADING	Addition to [PP-JCS]
OSP.OTA-SERVERS	Addition to [PP-JCS]
OSP.APSD-KEYS	Addition to [PP-JCS]
OSP.OPERATOR-KEYS	Addition to [PP-JCS]
OSP.KEY-GENERATION	Addition to [PP-JCS]
OSP.CASD-KEYS	Addition to [PP-JCS]
OSP.VASD-KEYS	Addition to [PP-JCS]
OSP.KEY-CHANGE	Addition to [PP-JCS]
OSP.SECURITY-DOMAINS	Addition to [PP-JCS]
OSP.QUOTAS	Addition to [PP-JCS]
OSP.URI-FILE-ACCESS	Addition to [PP-JCS] for SCWS

2.4.2.4 Assumptions

All assumptions of [PP-JCS] are included in this PP.

Assumptions	Conformance rationale with [PP-JCS]
A.MOBILE-OPERATOR	Addition to [PP-JCS] for card content management environment
A.OTA-ADMIN	Addition to [PP-JCS] for card content management environment
A.APPS-PROVIDER	Addition to [PP-JCS] for card content management environment
A.VERIFICATION-AUTHORITY	Addition to [PP-JCS] for card content management environment
A.KEY-ESCROW	Addition to [PP-JCS] for card content management environment
A.PERSONALIZER	Addition to [PP-JCS] for card content management environment
A.CONTROLLING-AUTHORITY	Addition to [PP-JCS] for card content management environment
A.PRODUCTION	Addition to [PP-JCS] for card content management environment

2.4.3 *Security Objectives*

In order to precisely state the relationship between the security objectives of the Java Card System and the security objectives for the SPD of this PP, the three notions defined for the SPD (equivalence, refinement and addition) in Section 2.4.2 will be used.

2.4.3.1 Security Objectives for the TOE

All Security Objectives of [PP-JCS] are included in this PP.

Security Objectives	Conformance rationale with [PP-JCS]
O.CARD-MANAGEMENT	Refinement of O.INSTALL, O.LOAD, O.DELETION and OE.CARD-MANAGEMENT from [PP-JCS].
O.DOMAIN-RIGHTS	Addition to [PP-JCS] for card content management environment
O.APPLI-AUTH	Refinement of O.LOAD from [PP-JCS].
O.COMM_AUTH	Addition to [PP-JCS] for card content management environment
O.COMM_INTEGRITY	Addition to [PP-JCS] for card content management environment
O.COMM_CONFIDENTIALITY	Addition to [PP-JCS] for card content management environment
O.INPUT-VALIDATION	Addition to [PP-JCS] for SCWS
O.DOS-DETECTION	Addition to [PP-JCS] for SCWS
O.REPLAY	Addition to [PP-JCS] for SCWS

2.4.3.2 Security Objectives for the Operational Environment

All Security Objectives for the Environment of [PP-JCS] are included in this PP, except OE.CARD-MANAGEMENT which is in this PP a refined security objective for the TOE.

Security Objectives	Conformance rationale with [PP-JCS]
OE.MOBILE-OPERATOR	Addition to [PP-JCS]
OE.OTA-ADMIN	Addition to [PP-JCS]
OE.APPS-PROVIDER	Addition to [PP-JCS]
OE.VERIFICATION-AUTHORITY	Addition to [PP-JCS]
OE.KEY-ESCROW	Addition to [PP-JCS]
OE.PERSONALIZER	Addition to [PP-JCS]
OE.CONTROLLING-AUTHORITY	Addition to [PP-JCS]
OE.PRODUCTION	Addition to [PP-JCS]
OE.SECURE-APPS-CERTIFICATION	Refinement of OE.VERIFICATION of [PP-JCS]
OE.BASIC-APPS-VALIDATION	Refinement of OE.VERIFICATION of [PP-JCS]
OE.AID-MANAGEMENT	Refinement of OE.VERIFICATION of [PP-JCS]
OE.OTA-LOADING	Addition to [PP-JCS]
OE.OTA-SERVERS	Addition to [PP-JCS]
OE.AP-KEYS	Addition to [PP-JCS]
OE.OPERATOR-KEYS	Addition to [PP-JCS]
OE.KEY-GENERATION	Addition to [PP-JCS]
OE.CA-KEYS	Addition to [PP-JCS]
OE.VA-KEYS	Addition to [PP-JCS]
OE.KEY-CHANGE	Addition to [PP-JCS]
OE.SECURITY-DOMAINS	Addition to [PP-JCS]
OE.QUOTAS	Addition to [PP-JCS]
OE.SHARE-CONTROL	Refinement of OE.VERIFICATION of [PP-JCS]
OE.SCP-SUPPORT	Equivalent to OE.SCP-SUPPORT of [PP-JCS]. Applies to SCWS and GP
OE.SCWS-ACP-ENFORCER	Addition to [PP-JCS] for SCWS

2.4.4 SFRs and SARs Statements Consistency

2.4.4.1 SFRs Consistency

The entire SFRs of the Java Card System are relevant to the TOE as defined in this PP.

All the operations performed on the Java Card SFRs are appropriate for the TOE since the TOE includes the full Java Card System.

Security Functional Requirements	Conformance rationale with [PP-JCS]
FDP_UIT.1/CCM	Addition to [PP-JCS]
FDP_ROL.1/CCM	Addition to [PP-JCS]
FDP_ITC.2/CCM	Addition to [PP-JCS]
FPT_FLS.1/CCM	Addition to [PP-JCS]
FCS_COP.1/DAP	Specific refinement of FCS_COP.1 of [PP-JCS] for DAP
FDP_ACC.1/SD	Addition to [PP-JCS] for card content management environment
FDP_ACF.1/SD	Addition to [PP-JCS] for card content management environment
FMT_MSA.1/SD	Addition to [PP-JCS] for card content management environment
FMT_MSA.3/SD	Addition to [PP-JCS] for card content management environment
FMT_SMF.1/SD	Addition to [PP-JCS] for card content management environment
FMT_SMR.1/SD	Addition to [PP-JCS] for card content management environment
FTP_ITC.1/SC	Refinement of FTP_ITC.1/CM of [PP-JCS]
FCO_NRO.2/SC	Refinement of FCO_NRO.2/CM of [PP-JCS]
FDP_IFC.2/SC	Refinement of FDP_IFF.1/CM of [PP-JCS]
FDP_IFF.1/SC	Refinement of FDP_IFF.1/CM of [PP-JCS]
FMT_MSA.1/SC	Addition for Secure Channel Protocol (SCP) IFC policy from FDP_IFC.2/SC
FMT_MSA.3/SC	Addition for Secure Channel Protocol (SCP) IFC policy from FDP_IFC.2/SC
FMT_SMF.1/SC	Addition for Secure Channel Protocol (SCP) IFC policy from FDP_IFC.2/SC
FIA_UID.1/SC	Refinement of FIA_UID.1/CM of [PP-JCS]
FIA_UAU.1/SC	Addition to [PP-JCS]
FIA_UAU.4/SC	Addition to [PP-JCS]
FPT_RPL.1/SCWS	Addition to [PP-JCS] for SCWS
FPT_FLS.1/SCWS	Addition to [PP-JCS] for SCWS
FPT_TDC.1/SCWS	Addition to [PP-JCS] for SCWS
FTP_TRP.1/SCWS	Addition to [PP-JCS] for SCWS
FTP_ITC.1/SCWS	Addition to [PP-JCS] for SCWS

2.4.4.2 SARs Consistency

This PP and the JCS PP share the same assurance level, that is EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

3 Security problem definition

3.1 Assets

Assets are security-relevant elements to be directly protected by the TOE. Confidentiality of assets is always intended with respect to un-trusted people or software, as various parties are involved during the first stages; details are given in threats hereafter.

They are divided first following the two configurations and then in two groups. The first one contains the data created by and for the user (User data) and the second one includes the data created by and for the TOE (TSF data). For each asset it is specified the kind of risks they run.

Note that assets listed in the underlying Java Card System Protection Profile are included in this Protection Profile. The ST writer shall take into account every asset of [PP-JCS].

3.1.1 Basic TOE

This section describes the assets for the Basic TOE configuration.

3.1.1.1 User Data

The following assets specialize the asset D.APP_KEYs from [PP-JCS].

D.APSD_KEYS

Application Provider Security Domains cryptographic keys needed to establish secure channels with the AP. These keys can be used to load and install applications on the card if the Security Domain has the appropriate privileges.

To be protected from unauthorized disclosure and modification.

D.CASD_KEYS

Controlling Authority Security Domains cryptographic keys needed to establish secure channels with the CA and to decrypt confidential content for APSDs.

To be protected from unauthorized disclosure and modification.

D.ISD_KEYS

Issuer Security Domain cryptographic keys needed to perform card management operations on the card.

To be protected from unauthorized disclosure and modification.

D.VASD_KEYS

Verification Authority Security Domain cryptographic keys needed to verify applications Mandated DAP signature.

To be protected from unauthorized disclosure and modification.

D.(U)SIM_DATA

Private data of the (U)SIM application, like the contents of its private fields.

To be protected from unauthorized disclosure and modification.

D.(U)SIM_CODE

The code of the (U)SIM application on the card.

To be protected from unauthorized modification.

3.1.1.2 TSF Data

D.GP_CODE

The code of the GlobalPlatform framework on the card.

To be protected from unauthorized modification.

D.CARD_MNGT_DATA

The data of the card management environment, like for instance, the identifiers, the privileges, life cycle states, the memory resource quotas of applets and security domains.

To be protected from unauthorized modification.

3.1.2 SCWS TOE

The assets for the SCWS TOE configuration consist of all the assets for Basic TOE plus the following assets.

3.1.2.1 User Data

D.SCWS_CODE

The code of the Smart Card Web Server (SCWS) on the card.

To be protected from unauthorized modification.

D.SCWS_AUTH

The secret data (PINs, passwords, runtime credentials such as cookies) used by the SCWS server to authenticate the User before providing him accessed to web pages controlled by access rights.

To be protected from unauthorized disclosure and modification.

3.1.2.2 TSF Data

D.SCWS_DATA

The data used by the SCWS server to control the access to the server and to servlets: - the resource protection set maintained by the SCWS server giving access rights on the URI server: access protocols (HTTP, HTTPS or remote administration protocol), users and authentication mode:

- the table of association maintained by the SCWS server mapping URL paths to the registered applications to be called if a request for one of these paths reaches the server.
- the Access Control Policy (ACP) data maintained by the SCWS to authenticate the mobile applications allowed to access the SCWS server. This data is loaded from the (U)SIM card by the mobile phone.

These data should be protected from unauthorized modification.

3.2 Users / Subjects

Subjects are active components of the TOE that (essentially) act on the behalf of users. Users of the TOE include people or institutions (like the AP, the MNO and the VA), hardware (like the CAD where the card is inserted) and software components (like the application packages installed on the card).

In this Protection Profile, relevant subjects are those listed in [PP-JCS] plus the following ones:

3.2.1 Basic TOE

This section describes the subjects for the Basic TOE configuration.

S.SD

A GlobalPlatform Security Domain representing on the card a off-card entity. This entity can be the Issuer, an Application Provider, the Controlling Authority or the Validation Authority.

3.2.2 SCWS TOE

The subjects for the SCWS TOE configuration consist of all the assets for Basic TOE plus the following assets.

S.SCWS_SERVLET

A content providing servlet that has been registered with the SCWS server.

S.SCWS_ADMIN_APPLET

The SCWS administration applet on the Java Card platform, receiving administration commands through BIP or OTA and communicating with the SCWS servlet.

3.3 Threats

This section introduces the threats to the assets against which specific protection within the TOE or its environment is required. Several groups of threats are distinguished according to the means used in the attack. The classification is also inspired by the components of the TOE that are supposed to counter each threat.

The threats listed below focus only on the (U)SIM Platform. Some of them refine those already present in [PP-JCS]. The ST writer shall take into account every threat of [PP-JCS] except those that have a [PP-JCS] equivalent in this PP according to the table in Section 2.4.2.2.

3.3.1 Basic TOE

This section describes threats for the Basic TOE configuration.

T.PHYSICAL

The attacker discloses or modifies the design of the TOE, its sensitive data or application code by physical (opposed to logical) tampering means. This threat includes IC failure analysis, electrical probing, unexpected tearing, and DPA. That also includes the modification of the TOE runtime execution through alteration of the intended execution order of (set of) instructions through physical tampering techniques.

This threatens all the identified assets.

T.INTEG-USER-DATA

The attacker through a malicious applet loaded on the card modifies application data, application keys or authentication data.

Directly threatened asset(s): **D.(U)SIM_DATA**, **D.ISD_KEYS**, **D.VASD_KEYS** **D.APSD_KEYS** and **D.CASD_KEYS**.

T.COM_EXPLOIT

An attacker remotely exploits the communication channel (USB, ISO-7816, NFC, BIP or SMS) established between the mobile phone and the (U)SIM card in order to modify or disclose confidential data.

All assets are threatened.

T.UNAUTHORIZED_CARD_MNGT

The attacker performs unauthorized card management operations (for instance impersonates one of the actor represented on the card) in order to take benefit of the privileges or services granted to this actor on the card such as fraudulent:

- load of a package file
- installation of a package file
- extradition of a package file or an applet
- personalization of an applet or a Security Domain
- deletion of a package file or an applet
- privileges update of an applet or a Security Domain

Directly threatened asset(s): **D.ISD_KEYS**, **D.CASD_KEYS**, **D.APSD_KEYS**, **D.APP_C_DATA** (from [PP-JCS]), **D.APP_I_DATA** (from [PP-JCS]), **D.APP_CODE** (from [PP-JCS]) and **D.CARD_MNGT_DATA**.

T.LIFE_CYCLE

An attacker accesses to an application outside of its expected availability range thus violating irreversible life cycle phases of the application (for instance, an attacker re-personalizes the application).

Directly threatened asset(s): **D.APP_I_DATA** (from [PP-JCS]), **D.APP_C_DATA** (from [PP-JCS]), and **D.CARD_MNGT_DATA**.

T.UNAUTHORIZED_ACCESS

By using the shareable object mechanism on which relies the communication between two applets, the attacker uses an applet on card to get access or to modify data from another applet that he should not have access to.

All assets are threatened.

3.3.2 SCWS TOE

The threats for the SCWS TOE configuration consist of all the threats for Basic TOE plus the following threats.

T.SCWS_FLAW

The SCWS servlet can contain breaches or vulnerabilities that could be remotely exploited by an attacker via HTTP requests, for instance in order to access to critical assets used by the servlet.

Directly threatened asset(s): **D.APP_I_DATA** (from [PP-JCS]), **D.APP_C_DATA** (from [PP-JCS]), **D.SCWS_CODE** and **D.SCWS_DATA**.

T.OBSOLETE_CONF

Because of the hard task in updating ACP (firewall) data and of the multiple mobile applications that could connect to the SCWS, the relevant data are outdated and:

- allow a malicious or vulnerable application to connect to the server;
- or allow an application signed with a revoked certificate to connect to the server;
- or prevents the user to connect using a legitimate application, but not recognized by the ACP data.

All assets are threatened.

T.REPLAY

The attacker captures the user's authentication cookie using monitoring software and replays it in a HTTP request to the application to gain access under a false identity.

Directly threatened assets: **D.SCWS_AUTH**.

T.DOS

An attacker prevents correct operation of the Java Card System through consumption of some resources of the card: RAM or NVRAM.

This threat, inherited from [PP-JCS], is extended to include remote attacks through the SCWS.

Directly threatened asset(s): **D.JCS_DATA** (see [PP-JCS]), **D.SCWS_DATA**

Application note:

For instance, the smart card could be attacked by a mobile application which sends multiple HTTP requests, causing its unavailability for other operations. This threat could be heightened by improper ACP data in the SCWS gateway, that would fail to block malicious or unknown mobile applications.

3.4 Organisational Security Policies

This section describes the organizational security policies to be enforced with respect to the TOE environment. Rules to which both the TOE and its human environment shall comply when addressing security needs related to (U)SIM Java Card Platform.

All the OSPs listed in [PP-JCS] are relevant for this Protection Profile. The ST writer shall take into account every OSP of [PP-JCS].

This Protection Profile adds the following OSPs:

3.4.1 Basic TOE

This section describes OSPs for the Basic TOE configuration.

3.4.1.1 Basic and Secure Applications Policies

This Protection Profile distinguishes basic from secure applets. The former must go through a validation process before being authorized to be load on the card. The latter are certified in composition with the current TOE and keep their certification independently of the other applets loaded on the card compliant with the following OSPs. Basic and Secure applets are loaded in different Java Card packages.

OSP.SECURE-APPS-CERTIFICATION

Secure applications must be certified according to the Common Criteria at an EAL equal to the one of the current Protection Profile.

The composition of these applications with the current PP must follow the rules defined in the document [Comp].

These applications are associated to a digital signature which will be checked by a VA during the loading into the TOE.

Application note:

This composition process requires that platform administrator and user guides (AGD_ADM and AGD_USR) are available to the secure application developer. The Evaluation report for the composition (ETR-COMP), delivered by the ITSEF which manages applications composition, must be also provided.

See [Secure APP] for more details on the evaluation/validation process.

OSP.BASIC-APPS-VALIDATION

Basic applications shall be associated to a digital signature which will be checked by a VA during the loading into the TOE.

In addition to the rules stated by the Java Card specification, the validation process must enforce that basic applications:

- must follow the extra-rules stated in the user manual of the considered (U)SIM Java Card Platform,
- cannot be libraries,
- must not use RMI,
- must not use proprietary libraries which are not certified (except system libraries),
- access control to certified proprietary libraries is controlled by the secure application which has defined the library,
- must be associated to an identifier and this identifier has to be used in parameter of the function calls.

Application note:

GSM file system and API's STK application descriptors are other ways to share object between applications.

Identifier usage allows to easily track applications calls. This is useful if a new attack path is discovered to identify the pieces of code that could be vulnerable.

See [Basic APP] for more details on the validation process.

OSP.SHARE-CONTROL

The Shareable interface functionality should be strictly controlled for all applications to prevent transitive data flows between applets (i.e., no resharing of a shareable object with a third applet) and thus prevent access to unauthorized data.

OSP.AID-MANAGEMENT

When loading an application that uses shareable object interface, to make its services available to other applications, the VA or the MNO shall verify that the AID of the application being loaded does not impersonate the AID known by another application on the card for the use of shareable services.

3.4.1.2 Loading Policies

OSP.OTA-LOADING

Application code, validated or certified depending on the application, is loaded "Over The Air" (OTA) onto (U)SIM Platform using OTA servers of the mobile operator.

If needed, the Card issuer can pre-authorize content loading operation through delegated management privilege to individual on-card representative of APs. In that case the application code is loaded in the APSD.

Once loaded, the application is personalized using the appropriate SD keys.

OSP.OTA-SERVERS

A security policy shall be employed by the mobile operator to ensure the security of the applications stored on its servers.

Application note:

The policy enforced by the mobile operator to ensure the security of the application can use mechanisms such as access control, isolation, regular check of integrity and encryption.

One possible realisation of this Organizational Security Policy is the enforcement of security rules defined in OTA servers security guidance document with regular site inspections to check the applicability of the rules.

3.4.1.3 Key Policies

OSP.APSD-KEYS

The APSD keys personalization can rely either on the key escrow if the APSD has been created before the usage phase of the (U)SIM card or on the CA if the APSD has been created during the usage phase.

In the first case, the security domain keys of the AP (APSD keys) are generated and stored in a secure way by the personalizer. Then, these keys are transmitted to the AP, via the key escrow, at the only mobile operator request.

In the second case, the APSD keys are:

- either generated and stored in a secure way by the APSD. Then these keys are securely transmitted to the AP using the CASD (Pull Model of [GP-CCCM]),
- or created by the AP and securely transfered to the APSD using the CASD (Push Model of [GP-CCCM]).

Generated keys must be unpredictable with use of an appropriate random source used in combination with appropriate pseudo-random techniques. Compromising the security of the key generation method shall require at least as many operations as determining the value of the generated key.

Application note:

For more details concerning this OSP, refer to [GP-CCCM].

OSP.OPERATOR-KEYS

The security of the mobile operator keys (ISD keys) must be ensured by a well defined security policy that covers generation, storage, distribution, destruction and recovery. This policy is enforced by the mobile operator in collaboration with the personalizer.

Application note:

Token keys used to verify the tokens included in Delegated Management commands (that embed the signature of these commands) must be different for each (U)SIM card in usage.

OSP.KEY-GENERATION

The personalizer must enforce a policy ensuring that generated keys cannot be accessed in plaintext.

Application note:

This can be applied by encrypting the generated key just after its generation with the public key of the recipient.

OSP.CASD-KEYS

The security domain keys of the CA must be securely generated and stored in the (U)SIM card during the personalization process. These keys are not modifiable after card issuance.

OSP.VASD-KEYS

The security domain keys of the VA must be securely generated and stored in the (U)SIM card during the personalization process.

3.4.1.4 Platform

OSP.KEY-CHANGE

The AP shall change its initial security domain keys (APSD) before any operation on its Security Domain.

3.4.1.5 GlobalPlatform

OSP.SECURITY-DOMAINS

Security domains can be dynamically created, deleted and blocked during usage phase in post-issuance mode.

OSP.QUOTAS

Security domains are subject to quotas of memory at creation.

3.4.2 SCWS TOE

The OSPs for the SCWS TOE configuration consist of all the OSPs for Basic TOE plus the following OSP.

OSP.URI-FILE-ACCESS

The optional feature provided by the SCWS which enables the access to the file system of the (U)SIM application via URIs shall be disabled.

3.5 Assumptions

The following assumption concerns the product operational environment, after product delivery. It applies to any kind of product, with Basic or SCWS TOE, that is, it holds in the Protection Profiles 09ya and 09yb.

All the assumptions mentioned in the [PP-JCS] Protection Profile are relevant. The ST writer shall take into account every assumption of [PP-JCS].

This Protection Profile adds the following assumptions:

3.5.1 Actors

A.MOBILE-OPERATOR

The mobile operator is a trusted actor responsible for the mobile network and the associated OTA servers.

The mobile operator as Card issuer cannot get access or change the application data which belongs to the AP.

A.OTA-ADMIN

Administrators of the mobile operator OTA servers are trusted people. They are trained to use and administrate securely those servers. They have the means and the equipments to perform their tasks.

They are aware of the sensitivity of the assets they managed and the responsibilities associated to the administration of OTA servers.

Application note:

OTA servers security guidance document with regular site inspections shall be employed to check the applicability of the rules.

A.APPS-PROVIDER

The AP is a trusted actor that provides basic or secure applications. He is responsible for his security domain keys (APSD keys).

Application note:

An AP generally refers to the entity that issues the application. For instance it can be a financial institution for a payment application such as EMV or a transport operator for a transport application such as Calypso.

A.VERIFICATION-AUTHORITY

The VA is a trusted actor who is able to guarantee and check the digital signature attached to a basic or secure application.

Application note:

As a consequence, it guarantees the success of the application validation or certification upon loading.

A.KEY-ESCROW

The key escrow is a trusted actor in charge of the secure storage of the initial AP keys generated by the TOE personalizer during initial personalization.

A.PERSONALIZER

The personalizer under an Operator's Contract is in charge of the TOE personalization process before card issuance. He ensures the security of the keys he loads on the (U)SIM cards:

- Mobile operator keys including OTA keys (telecom keys either generated by the personalizer or by the mobile operator) and delegated management token keys
- Issuer Security Domain keys (ISD keys or Card issuer keys),
- Application Provider Security Domains keys (APSD keys).
- Controlling Authority Security Domain keys (CASD keys)
- Verification Authority Security Domain keys (VASD keys)

A.CONTROLLING-AUTHORITY

The CA is a trusted actor responsible for securing the APSD keys creation and personalization. He is responsible for his security domain keys (CASD keys).

3.5.2 Secure Places

A.PRODUCTION

Production and personalization environment if the TOE delivery occurs before Phase 6 of the TOE life cycle must be trusted and secure.

4 Security Objectives

4.1 Security Objectives for the TOE

The security objectives of the TOE comprise the security objectives given in [PP-JCS], for the Java Card System, and the security objectives given hereafter, for the card management and for the SCWS in case of the SCWS TOE.

4.1.1 Basic TOE

This section describes the security objectives for the Basic TOE configuration.

The ST writer shall also include in its ST every security objective in [PP-JCS].

4.1.1.1 Card Management

O.CARD-MANAGEMENT

The TOE shall provide card management functionalities (loading, installation, extradition, deletion of applications and GP registry updates) in charge of the life cycle of the whole (U)SIM card and installed applications (applets)

The card manager, the application with specific rights responsible for the administration of the smart card, shall control the access to card management functions. It shall also implement the card issuer's policy on card management.

Application note:

The card manager will be tightly connected in practice with the rest of the TOE, which in return shall very likely rely on the card manager for the effective enforcement of some of its security functions.

The mechanism used to ensure authentication of the TOE issuer, that manages the TOE, or of the Service Providers owning a Security Domain with card management privileges is a secure channel. This channel will be used afterwards to protect commands exchanged with the TOE in confidentiality and integrity.

The platform guarantees that only the ISD or the Service Providers owning a Security Domain with the appropriate privilege (Delegated Management) can manage the applications on the card associated with its Security Domain. This is done accordingly with the card issuer's policy on card management.

The actor performing the operation must beforehand authenticate with the Security Domain. In the case of Delegated Management, the card management command will be associated with an electronic signature (GlobalPlatform token) verified by the ISD before execution.

O.DOMAIN-RIGHTS

The Card issuer shall not get access or change personalized AP security domain keys which belong to the AP. Modification of a security domain keyset is restricted to the AP who owns the security domain.

Application note:

APs have a set of keys that allows them to establish a secure channel between them and the platform. These keys sets are not known by the TOE issuer. The security domain initial keys are changed before any operation on the SD (OE.KEY-CHANGE) through standard PUT KEY procedures (if the initial keys were kept by key escrow) or through one of the SD personalization mechanisms described in Section 4.3.3 of [GP-UICC].

O.APPLI-AUTH

The card manager shall enforce the application security policies established by the card issuer by requiring application authentication during application loading on the card.

Application note:

Each application loaded onto the TOE has been signed by the VA. The VA will guarantee that the security policies established by the card issuer on applications are enforced. This authority is present on the TOE as a Security Domain whose role is to verify each signature at application loading.

The platform provides important extra features about application management and especially loading:

- Loaded applications are previously validated by an accredited laboratory for basic applications and certified by an accredited ITSEF for secure applications.
- All loaded applications are associated to a DAP signature generated by a VA which is verified at loading by the third party representative present on the platform (Mandated DAP verification).

4.1.1.2 Communication

O.COMM_AUTH

The TOE shall authenticate the origin of the card management requests that the card receives, and authenticate itself to the remote actor.

O.COMM_INTEGRITY

The TOE shall verify the integrity of the card management requests that the card receives.

O.COMM_CONFIDENTIALITY

The TOE shall be able to process card management requests containing encrypted data.

4.1.2 SCWS TOE

The security objectives for the SCWS TOE configuration consist of all the security objectives for Basic TOE plus the following security objectives.

O.INPUT-VALIDATION

HTTP requests received by the SCWS shall be checked for syntaxic validity and, for administrative requests, for integrity.

O.DOS-DETECTION

The SCWS shall detect Denial Of Service attacks attempts and be able to react in order to prevent (U)SIM card from overflooding.

O.REPLAY

The TOE must provide means of detection and rejection of the http replay attacks.

4.2 Security objectives for the Operational Environment

This section introduces the security objectives to be achieved by the environment associated to the TOE. The significant security objectives for the environment of the TOE are the ones linked to relevant assumptions and OSPs.

The ST writer shall include in its ST all the security objectives for the environment of the Java Card System Protection Profile [PP-JCS] except:

- the card management security objective which is now part of the TOE. Hence, the objective for the environment OE.CARD-MANAGEMENT from [PP-JCS] shall not appear in a ST based on this PP.
- OE.SCP-SUPPORT from [PP-JCS] which is replaced by the equivalent OE.SCP-SUPPORT from this PP.

4.2.1 Basic TOE

This section describes the security objectives for the operational environment for the Basic TOE configuration

4.2.1.1 Actors

OE.MOBILE-OPERATOR

The mobile operator shall be a trusted actor responsible for the mobile network and the associated OTA servers.

OE.OTA-ADMIN

Administrators of the mobile operator OTA servers shall be trusted people. They shall be trained to use and administrate those servers. They have the means and the equipments to perform their tasks.

They must be aware of the sensitivity of the assets they manage and the responsibilities associated to the administration of OTA servers.

Application note:

One possible realisation of this assumption is the enforcement of security rules defined in an OTA servers security guidance document with regular site inspections to check the applicability of the rules

OE.APPS-PROVIDER

The AP shall be a trusted actor that provides basic or secure application. He must be responsible of his security domain keys.

OE.VERIFICATION-AUTHORITY

The VA should be a trusted actor who is able to guarantee and check the digital signature attached to an application.

OE.KEY-ESCROW

The key escrow shall be a trusted actor in charge of the secure storage of the AP initial keys generated by the personalizer.

OE.PERSONALIZER

The personalizer shall be a trusted actor in charge of the personalization process. He must ensure the security of the keys it manages and loads into the card:

- Mobile operator keys including OTA keys (telecom keys either generated by the personalizer or by the mobile operator),
- Issuer Security Domain keys (ISD keys),
- Application Provider Security Domain keys (APSD keys).
- Controlling Authority Security Domain keys (CASD keys)

OE.CONTROLLING-AUTHORITY

The CA shall be a trusted actor responsible for securing the APSD keys creation and personalisation. He must be responsible for his security domain keys (CASD keys).

4.2.1.2 Secure places

OE.PRODUCTION

Production and personalization environment if the TOE delivery occurs before Phase 6 of the TOE life cycle must be trusted and secure.

4.2.1.3 Policies

Validation and Certification

OE.SECURE-APPS-CERTIFICATION

Secure applications must be evaluated and certified at a security level higher or equal than the one of the current Protection Profile.

OE.BASIC-APPS-VALIDATION

Basic applications must be analysed during the validation process in order to ensure that the rules for correct usage of the TOE are still enforced.

OE.AID-MANAGEMENT

The VA or the MNO shall verify that the AID of the application being loaded does not impersonate the AID known by another application on the card for the use of shareable services.

Loading

OE.OTA-LOADING

Application code, validated or certified depending on the application, is loaded "Over The Air" (OTA) onto (U)SIM Platform using OTA servers. This process should protect the confidentiality and the integrity of the loaded application code.

OE.OTA-SERVERS

The mobile operator must enforce a policy to ensure the security of the applications stored on its servers.

Keys

OE.AP-KEYS

The SD keys personalizer, the AP and the key escrow must enforce a security policy on SD keys in order to secure their transmission.

OE.OPERATOR-KEYS

The security of the mobile operator keys must be ensured in the environment of the TOE.

OE.KEY-GENERATION

The personalizer must ensure that the generated keys cannot be accessed by unauthorized users.

OE.CA-KEYS

The security domain keys of the CA must be securely generated prior storage in the (U)SIM card.

OE.VA-KEYS

The security domain keys of the VA must be securely generated prior storage in the (U)SIM card.

4.2.1.4 Platform

OE.KEY-CHANGE

The AP must change its security domain initial keys before any operation on it.

4.2.1.5 GlobalPlatform

OE.SECURITY-DOMAINS

Security domains can be dynamically created, deleted and blocked during usage phase in post-issuance mode.

OE.QUOTAS

Security domains are subject to quotas of memory at creation.

4.2.1.6 Applications

OE.SHARE-CONTROL

All applications (basic and secure applications) must have means to identify the applications with whom they share data using the Shareable Interface.

Application note:

If an application implementing a Shareable Interface has to share data with a new application, it has to be updated, and thus re-validated, to take into account the identification of this new application (through its AID for instance) before sharing data.

4.2.1.7 SCP

OE.SCP-SUPPORT

The TOE OS shall support the following functionalities:

- (1) It does not allow the TSFs to be bypassed or altered and does not allow access to other low-level functions than those made available by the packages of the API. That includes the protection of its private data and code (against disclosure or modification) from the Java Card System.
- (2) It provides secure low-level cryptographic processing to the Java Card System, GlobalPlatform and SCWS frameworks (for SCWS TOE).
- (3) It supports the needs for any update to a single persistent object or class field to be atomic, and possibly a low-level transaction mechanism.
- (4) It allows the Java Card System to store data in "persistent technology memory" or in volatile memory, depending on its needs (for instance, transient objects must not be stored in non-volatile memory). The memory model is structured and allows for low-level control accesses (segmentation fault detection).

4.2.2 SCWS TOE

The security objectives for the operational environment for the SCWS TOE configuration consist of all the security objectives for the operational environment for Basic TOE plus the following security objectives for the operational environment.

OE.SCWS-ACP-ENFORCER

The mobile phone connected to the (U)SIM card shall support in its SCWS gateway the ACP (Access Control Policy) enforcer functionality defined in SCWS specifications. This optional feature of the SCWS, particularly useful for mobile phones with open operating systems, limits the access of mobile applications to the SCWS. ACP data is retrieved by the mobile phone from the SCWS server. Furthermore, regular updates of the ACP data maintained by the SCWS server shall be made. They should decrease neither the security nor the functionalities of previous versions.

Application note:

It is recommended that the (U)SIM card supports the storage of the configuration file ('/ config / acp') required for the firewall.

OE.URI-FILE-ACCESS

The optional feature provided by the SCWS which enables the access to the file system of the (U)SIM application via URIs should be disabled because it provides a means of complementary access to those files and thus it can be a source of vulnerabilities.

4.3 Security Objectives Rationale

4.3.1 Threats

4.3.1.1 Basic TOE

T.PHYSICAL This threat is countered by physical protections which rely on the underlying platform and are therefore an environmental issue.

The security objectives OE.SCP-SUPPORT and OE.SCP-IC (from [PP-JCS]) protect sensitive assets of the platform against loss of integrity and confidentiality and especially ensure the TSFs cannot be bypassed or altered.

T.INTEG-USER-DATA The security objective OE.SCP-SUPPORT provides functionality to ensure atomicity of sensitive operations, secure low level access control and protection against bypassing of the security features of the TOE. In particular, it explicitly ensures the independent protection in integrity of the platform data.

The security objectives O.DOMAIN-RIGHTS, OE.CA-KEYS, OE.VA-KEYS and OE.AP-KEYS ensure that personalization of the application by its associated security domain is only performed by the authorized AP.

The security objectives from [PP-JCS] covering the threat T.INTEG-APPLI-DATA also cover this threat.

T.COM_EXPLOIT This threat is covered by the following security objectives:

- O.COMM_AUTH prevents unauthorized users from initiating a malicious card management operation.
- O.COMM_INTEGRITY protects the integrity of the card management data while it is in transit to the (U)SIM card.
- O.COMM_CONFIDENTIALITY prevents from disclosing encrypted data transiting to the (U)SIM card.

T.UNAUTHORIZED_CARD_MNGT This threat is covered by the following security objectives:

- O.CARD-MANAGEMENT controls the access to card management functions such as the loading, installation, extradition or deletion of applets.
- O.COMM_AUTH prevents unauthorized users from initiating a malicious card management operation.
- O.COMM_INTEGRITY protects the integrity of the card management data while it is in transit to the (U)SIM card.
- O.APPLI-AUTH which requires for loading all applications to be authenticated.
- O.DOMAIN-RIGHTS which restricts the modification of an AP security domain keyset to the AP who owns it.

T.LIFE_CYCLE This threat is covered by the security objectives:

- O.CARD-MANAGEMENT that controls the access to card management functions such as the loading, installation, extradition or deletion of applets and prevent attacks intended to modify or exploit the current life cycle of applications

- O.DOMAIN-RIGHTS that restricts the use of an AP security domain keysets, and thus the management of the applications related to this SD, to the AP who owns it.

T.UNAUTHORIZED_ACCESS This threat is covered by the security objective on the operational environment of the TOE OE.SHARE-CONTROL which ensures that sharing objects functionality is strictly controlled to stop data transitive flows between applets and thus stop access to unauthorized data.

4.3.1.2 SCWS TOE

T.SCWS_FLAW This threat is countered by the security objectives:

- O.INPUT-VALIDATION which ensures that the syntax of HTTP(s) requests can not be harmful;
- O.APPLI-AUTH which ensures that only authentified applications (including SCWS applications) that have followed a validation according to a security policy (OE.BASIC-APPS-VALIDATION) have been loaded on the card;
- O.REPLAY that detects possible replay attacks that could be used to abuse the SCWS server.

T.OBSOLETE_CONF This threat is countered by the environment security objective OE.SCWS-ACP-ENFORCER which ensures that the ACP enforcer functionality is present on the mobile and that regular updates of the ACP data are made.

T.REPLAY This threat is countered by the security objective O.REPLAY which ensures that the http replay attacks are detected and rejected.

T.DOS This threat is countered by the security objective on the OS OE.SCP-SUPPORT, the following security objectives on the Java Card System: O.INSTALL, O.OPERATE and O.RESSOURCES (see [PP-JCS]), the security objective on the IC OE.SCP.RECOVERY (see [PP-JCS]) and the security objective O.DOS-DETECTION which counters Denial Of Service attacks in order to prevent (U)SIM card from overflooding.

4.3.2 Organisational Security Policies

4.3.2.1 Basic TOE

Basic and Secure Applications Policies

OSP.SECURE-APPS-CERTIFICATION This OSP is enforced by the security objective for the operational environment of the TOE OE.SECURE-APPS-CERTIFICATION.

OSP.BASIC-APPS-VALIDATION This OSP is enforced by the security objective for the operational environment of the TOE OE.BASIC-APPS-VALIDATION.

OSP.SHARE-CONTROL This OSP is directly enforced by the security objective for the operational environment of the TOE OE.SHARE-CONTROL.

OSP.AID-MANAGEMENT This OSP is directly enforced by the security objective for the operational environment of the TOE OE.AID-MANAGEMENT.

Loading Policies

OSP.OTA-LOADING This OSP is enforced by the security objective for the operational environment of the TOE OE.OTA-LOADING.

OSP.OTA-SERVERS This OSP is enforced by the security objective for the operational environment of the TOE OE.OTA-SERVERS.

Key Policies

OSP.APSD-KEYS This OSP is enforced by the security objective for the operational environment of the TOE OE.AP-KEYS.

OSP.OPERATOR-KEYS This OSP is enforced by the security objective for the operational environment of the TOE OE.OPERATOR-KEYS.

OSP.KEY-GENERATION This OSP is enforced by the security objective for the operational environment of the TOE OE.KEY-GENERATION.

OSP.CASD-KEYS This OSP is enforced by the security objective for the operational environment of the TOE OE.CA-KEYS.

OSP.VASD-KEYS This OSP is enforced by the security objective for the operational environment of the TOE OE.VA-KEYS.

Platform

OSP.KEY-CHANGE This OSP is enforced by the security objective for the operational environment of the TOE OE.KEY-CHANGE.

GlobalPlatform

OSP.SECURITY-DOMAINS This OSP is enforced by the security objective for the operational environment of the TOE OE.SECURITY-DOMAINS.

OSP.QUOTAS This OSP is enforced by the security objective for the operational environment of the TOE OE.QUOTAS.

4.3.2.2 SCWS TOE

OSP.URI-FILE-ACCESS This OSP is enforced by the security objective for the operational environment of the TOE OE.URI-FILE-ACCESS.

4.3.3 Assumptions

4.3.3.1 Actors

A.MOBILE-OPERATOR This assumption is directly upheld by OE.MOBILE-OPERATOR.

A.OTA-ADMIN This assumption is directly upheld by OE.OTA-ADMIN.

A.APPS-PROVIDER This assumption is directly upheld by OE.APPS-PROVIDER.

A.VERIFICATION-AUTHORITY This assumption is directly upheld by OE.VERIFICATION-AUTHORITY.

A.KEY-ESCROW This assumption is directly upheld by OE.KEY-ESCROW.

A.PERSONALIZER This assumption is directly upheld by OE.PERSONALIZER.

A.CONTROLLING-AUTHORITY This assumption is directly upheld by OE.CONTROLLING-AUTHORITY.

4.3.3.2 Secure Places

A.PRODUCTION This assumption is directly upheld by OE.PRODUCTION.

4.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.PHYSICAL	OE.SCP-SUPPORT	Section 4.3.1
T.INTEG-USER-DATA	O.DOMAIN-RIGHTS, OE.SCP-SUPPORT, OE.CA-KEYS, OE.AP-KEYS, OE.VA-KEYS	Section 4.3.1
T.COM_EXPLOIT	O.COMM_AUTH, O.COMM_INTEGRITY, O.COMM_CONFIDENTIALITY	Section 4.3.1
T.UNAUTHORIZED_CARD_MNGT	O.CARD-MANAGEMENT, O.COMM_AUTH, O.COMM_INTEGRITY, O.APPLI-AUTH, O.DOMAIN-RIGHTS	Section 4.3.1
T.LIFE_CYCLE	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS	Section 4.3.1
T.UNAUTHORIZED_ACCESS	OE.SHARE-CONTROL	Section 4.3.1
T.SCWS_FLAW	O.INPUT-VALIDATION, O.REPLAY, O.APPLI-AUTH, OE.BASIC-APPS-VALIDATION	Section 4.3.1
T.OBSOLETE_CONF	OE.SCWS-ACP-ENFORCER	Section 4.3.1
T.REPLAY	O.REPLAY	Section 4.3.1
T.DOS	O.DOS-DETECTION, OE.SCP-SUPPORT	Section 4.3.1

Table 1 Threats and Security Objectives - Coverage

Security Objectives	Threats
O.CARD-MANAGEMENT	T.UNAUTHORIZED_CARD_MNGT, T.LIFE_CYCLE
O.DOMAIN-RIGHTS	T.INTEG-USER-DATA, T.UNAUTHORIZED_CARD_MNGT, T.LIFE_CYCLE
O.APPLI-AUTH	T.UNAUTHORIZED_CARD_MNGT, T.SCWS_FLAW
O.COMM_AUTH	T.COM_EXPLOIT, T.UNAUTHORIZED_CARD_MNGT
O.COMM_INTEGRITY	T.COM_EXPLOIT, T.UNAUTHORIZED_CARD_MNGT
O.COMM_CONFIDENTIALITY	T.COM_EXPLOIT
O.INPUT-VALIDATION	T.SCWS_FLAW
O.DOS-DETECTION	T.DOS
O.REPLAY	T.SCWS_FLAW, T.REPLAY
OE.MOBILE-OPERATOR	
OE.OTA-ADMIN	
OE.APPS-PROVIDER	
OE.VERIFICATION-AUTHORITY	
OE.KEY-ESCROW	
OE.PERSONALIZER	
OE.CONTROLLING-AUTHORITY	
OE.PRODUCTION	
OE.SECURE-APPS-CERTIFICATION	
OE.BASIC-APPS-VALIDATION	T.SCWS_FLAW
OE.AID-MANAGEMENT	
OE.OTA-LOADING	
OE.OTA-SERVERS	
OE.AP-KEYS	T.INTEG-USER-DATA
OE.OPERATOR-KEYS	
OE.KEY-GENERATION	
OE.CA-KEYS	T.INTEG-USER-DATA
OE.VA-KEYS	T.INTEG-USER-DATA

Security Objectives	Threats
OE.KEY-CHANGE	
OE.SECURITY-DOMAINS	
OE.QUOTAS	
OE.SHARE-CONTROL	T.UNAUTHORIZED_ACCESS
OE.SCP-SUPPORT	T.PHYSICAL, T.INTEG-USER-DATA, T.DOS
OE.SCWS-ACP-ENFORCER	T.OBSOLETE_CONF
OE.URI-FILE-ACCESS	

Table 2 Security Objectives and Threats - Coverage

Organisational Security Policies	Security Objectives	Rationale
OSP.SECURE-APPS-CERTIFICATION	OE.SECURE-APPS-CERTIFICATION	Section 4.3.2
OSP.BASIC-APPS-VALIDATION	OE.BASIC-APPS-VALIDATION	Section 4.3.2
OSP.SHARE-CONTROL	OE.SHARE-CONTROL	Section 4.3.2
OSP.AID-MANAGEMENT	OE.AID-MANAGEMENT	Section 4.3.2
OSP.OTA-LOADING	OE.OTA-LOADING	Section 4.3.2
OSP.OTA-SERVERS	OE.OTA-SERVERS	Section 4.3.2
OSP.APSD-KEYS	OE.AP-KEYS	Section 4.3.2
OSP.OPERATOR-KEYS	OE.OPERATOR-KEYS	Section 4.3.2
OSP.KEY-GENERATION	OE.KEY-GENERATION	Section 4.3.2
OSP.CASD-KEYS	OE.CA-KEYS	Section 4.3.2
OSP.VASD-KEYS	OE.VA-KEYS	Section 4.3.2
OSP.KEY-CHANGE	OE.KEY-CHANGE	Section 4.3.2
OSP.SECURITY-DOMAINS	OE.SECURITY-DOMAINS	Section 4.3.2
OSP.QUOTAS	OE.QUOTAS	Section 4.3.2
OSP.URI-FILE-ACCESS	OE.URI-FILE-ACCESS	Section 4.3.2

Table 3 OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies
O.CARD-MANAGEMENT	
O.DOMAIN-RIGHTS	
O.APPLI-AUTH	
O.COMM_AUTH	
O.COMM_INTEGRITY	
O.COMM_CONFIDENTIALITY	
O.INPUT-VALIDATION	
O.DOS-DETECTION	
O.REPLAY	
OE.MOBILE-OPERATOR	
OE.OTA-ADMIN	
OE.APPS-PROVIDER	
OE.VERIFICATION-AUTHORITY	
OE.KEY-ESCROW	
OE.PERSONALIZER	
OE.CONTROLLING-AUTHORITY	
OE.PRODUCTION	
OE.SECURE-APPS-CERTIFICATION	OSP.SECURE-APPS-CERTIFICATION
OE.BASIC-APPS-VALIDATION	OSP.BASIC-APPS-VALIDATION
OE.AID-MANAGEMENT	OSP.AID-MANAGEMENT
OE.OTA-LOADING	OSP.OTA-LOADING
OE.OTA-SERVERS	OSP.OTA-SERVERS
OE.AP-KEYS	OSP.APSD-KEYS
OE.OPERATOR-KEYS	OSP.OPERATOR-KEYS
OE.KEY-GENERATION	OSP.KEY-GENERATION
OE.CA-KEYS	OSP.CASD-KEYS
OE.VA-KEYS	OSP.VASD-KEYS
OE.KEY-CHANGE	OSP.KEY-CHANGE
OE.SECURITY-DOMAINS	OSP.SECURITY-DOMAINS
OE.QUOTAS	OSP.QUOTAS
OE.SHARE-CONTROL	OSP.SHARE-CONTROL
OE.SCP-SUPPORT	
OE.SCWS-ACP-ENFORCER	

Security Objectives	Organisational Security Policies
OE.URI-FILE-ACCESS	OSP.URI-FILE-ACCESS

Table 4 Security Objectives and OSPs - Coverage

Assumptions	Security objectives for the Operational Environment	Rationale
A.MOBILE-OPERATOR	OE.MOBILE-OPERATOR	Section 4.3.3
A.OTA-ADMIN	OE.OTA-ADMIN	Section 4.3.3
A.APPS-PROVIDER	OE.APPS-PROVIDER	Section 4.3.3
A.VERIFICATION-AUTHORITY	OE.VERIFICATION-AUTHORITY	Section 4.3.3
A.KEY-ESCROW	OE.KEY-ESCROW	Section 4.3.3
A.PERSONALIZER	OE.PERSONALIZER	Section 4.3.3
A.CONTROLLING-AUTHORITY	OE.CONTROLLING-AUTHORITY	Section 4.3.3
A.PRODUCTION	OE.PRODUCTION	Section 4.3.3

Table 5 Assumptions and Security Objectives for the Operational Environment - Coverage

Security objectives for the Operational Environment	Assumptions
OE.MOBILE-OPERATOR	A.MOBILE-OPERATOR
OE.OTA-ADMIN	A.OTA-ADMIN
OE.APPS-PROVIDER	A.APPS-PROVIDER
OE.VERIFICATION-AUTHORITY	A.VERIFICATION-AUTHORITY
OE.KEY-ESCROW	A.KEY-ESCROW
OE.PERSONALIZER	A.PERSONALIZER
OE.CONTROLLING-AUTHORITY	A.CONTROLLING-AUTHORITY
OE.PRODUCTION	A.PRODUCTION
OE.SECURE-APPS-CERTIFICATION	
OE.BASIC-APPS-VALIDATION	
OE.AID-MANAGEMENT	
OE.OTA-LOADING	
OE.OTA-SERVERS	
OE.AP-KEYS	
OE.OPERATOR-KEYS	
OE.KEY-GENERATION	
OE.CA-KEYS	
OE.VA-KEYS	
OE.KEY-CHANGE	
OE.SECURITY-DOMAINS	
OE.QUOTAS	
OE.SHARE-CONTROL	
OE.SCP-SUPPORT	
OE.SCWS-ACP-ENFORCER	
OE.URI-FILE-ACCESS	

Table 6 Security Objectives for the Operational Environment and Assumptions - Coverage

5 Security Functional Requirements

5.1 Security Functional Requirements

This section describes the requirements imposed on the TOE in order to achieve the security objectives laid down in the previous chapter. All the requirements identified in this section are instances of those stated in [CC2].

All the Java Card System Platform security functional requirements are relevant for this Protection Profile.

The SFRs listed below state requirements specific to the (U)SIM Platform.

5.1.1 Basic TOE

This section describes the SFR for the Basic TOE configuration.

5.1.1.1 Card Manager (CMGRG)

This section contains the security requirements for the card manager.

The security requirements below help to define a policy for controlling access to card content management operations and for expressing card issuer security concerns. Most of them come from [JCS] but are instantiated to add more precisions regarding (U)SIM card content management. This policy depends on the particular security and card management architecture present in the card. Therefore the policy shall be instantiated when developing conformant Security Targets.

Card Content Management

FDP_UIT.1/CCM Data exchange integrity

FDP_UIT.1.1/CCM The TSF shall enforce the **Secure Channel Protocol information flow control policy and the Security Domain access control policy** to **receive** user data in a manner protected from **modification, deletion, insertion and replay** errors.

FDP_UIT.1.2/CCM The TSF shall be able to determine on receipt of user data, whether **[selection: modification, deletion, insertion, replay]** has occurred.

FDP_ROL.1/CCM Basic rollback

FDP_ROL.1.1/CCM The TSF shall enforce **Security Domain access control policy** to permit the rollback of the **installation operation** on the **executable files and application instances**.

FDP_ROL.1.2/CCM The TSF shall permit operations to be rolled back within the **[assignment: boundary limit to which rollback may be performed]**.

FDP_ITC.2/CCM Import of user data with security attributes

FDP_ITC.2.1/CCM The TSF shall enforce the **Firewall access control policy and the Secure Channel Protocol information flow policy** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.2.2/CCM The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3/CCM The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4/CCM The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5/CCM The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[assignment: additional importation control rules]**.

Application note:

This Functional Component Instance enforces a security information flow control policy. Rules must be defined for importation operations. These rules must take into account all user data.

FPT_FLS.1/CCM Failure with preservation of secure state

FPT_FLS.1.1/CCM The TSF shall preserve a secure state when the following types of failures occur: **the Security Domain fails to load/install an Executable File / application instance as described in [JCRE], Section 11.3.4**.

FCS_COP.1/DAP Cryptographic operation

FCS_COP.1.1/DAP The TSF shall perform **verification of the DAP signature attached to Executable Load Applications** in accordance with a specified cryptographic algorithm

- **PKC Scheme: SHA-1 hash and PKCS#1 RSA signature**
- **or DES Scheme: Single DES plus final Triple DES MAC (Retail MAC)**

and cryptographic key sizes

- **PKC Scheme: RSA key of minimum length 1024 bits**
- **DES Scheme: DES key of miminim length 16 bytes**

that meet the following:

- **Sections C.1.2 and C.6 of [GP]**
- **PKC Scheme: SSA-PKCS1-v1_5 as defined in PKCS#1**
- **DES Scheme: ISO 9797-1 as MAC Algorithm 3 with output transformation 3, without truncation, and with DES taking the place of the block cipher**
- **[assignment: national requirements for cryptographic algorithms]**.

Security Domain

FDP_ACC.1/SD Subset access control

FDP_ACC.1.1/SD The TSF shall enforce the **Security Domain access control policy** on:

- **Subjects: S.INSTALLER, S.ADEL, S.CAD (from [PP-JCS]) and S.SD**
- **Objects: Delegation Token, DAP Block and Load File**
- **Operations: GlobalPlatform's card content management APDU commands and API methods.**
- **[assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]**.

FDP_ACF.1/SD Security attribute based access control

FDP_ACF.1.1/SD The TSF shall enforce the **Security Domain access control policy** to objects based on the following:

- **Subjects:**
  - **S.INSTALLER, defined in [PP-JCS] and represented by the GlobalPlatform Environment (OPEN) on the card, the Card Life Cycle attributes (defined in Section 5.1.1 of [GP]);**
  - **S.ADEL, also defined in [PP-JCS] and represented by the GlobalPlatform Environment (OPEN) on the card;**
  - **S.SD receiving the Card Content Management commands (through APDUs or APIs) with a set of privileges (defined in Section 6.6.1 of [GP]), a life-cycle status (defined in Section 5.3.2 of [GP]) and a**

Secure Communication Security level (defined in Section 10.6 of [GP]);

  - **S.CAD, defined in [PP-JCS], the off-card entity that communicates with the S.INSTALLER through S.SD;**

- **Objects:**
  - **The Delegation Token, in case of Delegated Management operations, with the attributes Present or Not Present;**
  - **The DAP Block, in case of application loading, with the attributes Present or Not Present;**
  - **The Load File or Executable File, in case of application loading, installation, extradition or registry update, with a set of intended privileges and its targeted associated SD AID.**
- **[assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]**.

FDP_ACF.1.2/SD The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

Runtime behavior rules defined by GlobalPlatform for:

- **loading (Section 9.3.5 of [GP]);**
- **installation (Section 9.3.6 of [GP]);**
- **extradition (Section 9.4.1 of [GP]);**
- **registry update (Section 9.4.2 of [GP]);**
- **content removal (Section 9.5 of [GP])**.

FDP_ACF.1.3/SD The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]**.

FDP_ACF.1.4/SD The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **following rule: when at least one of the rules defined by GlobalPlatform does not hold**.

FMT_MSA.1/SD Management of security attributes

FMT_MSA.1.1/SD The TSF shall enforce the **Security Domain access control policy** to restrict the ability to **modify** the security attributes **[assignment: list of security attributes]** to **the Security Domain and the application instance itself**.

FMT_MSA.3/SD Static attribute initialisation

FMT_MSA.3.1/SD The TSF shall enforce the **Security Domain access control policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/SD The TSF shall allow the **[assignment: the authorised identified roles]** to specify alternative initial values to override the default values when an object or information is created.

Refinement:

Alternative initial values shall be at least as restrictive as the default values defined in FMT_MSA.3.1.

FMT_SMF.1/SD Specification of Management Functions

FMT_SMF.1.1/SD The TSF shall be capable of performing the following management functions: **[assignment: list of management functions to be provided by the TSF]**.

FMT_SMR.1/SD Security roles

FMT_SMR.1.1/SD The TSF shall maintain the roles **[assignment: the authorised identified roles]**.

FMT_SMR.1.2/SD The TSF shall be able to associate users with roles.

Secure Channel

FTP_ITC.1/SC Inter-TSF trusted channel

FTP_ITC.1.1/SC The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/SC The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/SC The TSF shall initiate communication via the trusted channel for **all card management functions:**

- **loading;**
- **installation;**
- **extradition;**

- **registry update;**
- **SD personalization;**
- **[assignment: list of functions for which a trusted channel is required]**.

FCO_NRO.2/SC Enforced proof of origin

FCO_NRO.2.1/SC The TSF shall enforce the generation of evidence of origin for transmitted **Executable load files** at all times.

FCO_NRO.2.2/SC The TSF shall be able to relate the **[assignment: list of attributes]** of the originator of the information, and the **identity** of the information to which the evidence applies.

FCO_NRO.2.3/SC The TSF shall provide a capability to verify the evidence of origin of information to **originator** given **Executable load files**.

FDP_IFC.2/SC Complete information flow control

FDP_IFC.2.1/SC The TSF shall enforce the **Secure Channel Protocol information flow control policy** on

- **the subjects S.CAD and S.SD, involved in the exchange of messages between the (U)SIM card and the CAD through a potentially unsafe communication channel**
- **the information controlled by this policy is the card content management command, including personalization commands, in the APDUs sent to the card and their associated responses returned to the CAD.**
- **[assignment: list of subjects and information]**

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2/SC The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

FDP_IFF.1/SC Simple security attributes

FDP_IFF.1.1/SC The TSF shall enforce the **Secure Channel Protocol information flow control policy** based on the following types of subject and information security attributes:

- **Subjects:**
  - **S.SD receiving the Card Content Management commands (through APDUs or APIs). This subject can be the ISD, an APSD or a CASD.**

    - **S.CAD the off-card entity that communicates with the S.SD.**
  - **Information:**
    - **load file, in case of application loading;**
    - **applications or SD privileges, in case of application installation or registry update;**
    - **personalization keys and/or certificates, in case of application or SD personnalization.**
  - **[assignment: list of subjects and information controlled under the indicated SFP, and for each, the security attributes]**.

FDP_IFF.1.2/SC The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- **Runtime behavior rules defined by GlobalPlatform for:**
  - **loading (Section 9.3.5 of [GP]);**
  - **installation (Section 9.3.6 of [GP]);**
  - **extradition (Section 9.4.1 of [GP]);**
  - **registry update (Section 9.4.2 of [GP]);**
  - **SD personalization rules, pull and push models (Section 11 of [GP-UICC]).**
- **[assignment: for each operation, the security attribute-based relationship that must hold between subject and information security attributes]**.

FDP_IFF.1.3/SC The TSF shall enforce the **[assignment: additional information flow control SFP rules]**.

FDP_IFF.1.4/SC The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: rules, based on security attributes, that explicitly authorise information flows]**.

FDP_IFF.1.5/SC The TSF shall explicitly deny an information flow based on the following rules:

- **When none of the conditions listed in the element FDP_IFF.1.4 of this component hold and at least one of those listed in the element FDP_IFF.1.2 does not hold**.

Application note:

The on-card and the off-card subjects have security attributes such as MAC, Cryptogram, Challenge, Key Set, Static Keys, etc.

FMT_MSA.1/SC Management of security attributes

FMT_MSA.1.1/SC The TSF shall enforce the **Secure Channel Protocol (SCP) information flow control policy** to restrict the ability to **modify** the security attributes

[assignment: list of security attributes] to **[assignment: the authorised identified roles]**.

Application note:

The authorized identified roles could be the card issuer (off-card) or a SD (on-card).

FMT_MSA.3/SC Static attribute initialisation

FMT_MSA.3.1/SC The TSF shall enforce the **Secure Channel Protocol (SCP) information flow control policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2/SC The TSF shall allow the **[assignment: the authorised identified roles]** to specify alternative initial values to override the default values when an object or information is created.

Refinement:

Alternative initial values shall be at least as restrictive as the default values defined in FMT_MSA.3.1.

FMT_SMF.1/SC Specification of Management Functions

FMT_SMF.1.1/SC The TSF shall be capable of performing the following management functions:

- **Management functions specified in GlobalPlatform specifications [GP]:**
  - **loading (Section 9.3.5 of [GP]);**
  - **installation (Section 9.3.6 of [GP]);**
  - **extradition (Section 9.4.1 of [GP]);**
  - **registry update (Section 9.4.2 of [GP]);**
  - **SD personalization rules, pull and push models (Section 11 of [GP-UICC]).**
- **[assignment: list of management functions to be provided by the TSF]**.

Application note:

All management functions related to SCP02 secure channel shall be relevant.

FIA_UID.1/SC Timing of identification

FIA_UID.1.1/SC The TSF shall allow

- **application selection;**
- **initializing a secure channel with the card;**
- **requesting data that identifies the card or the Card Issuer;**

- **[assignment: list of TSF-mediated actions]**

on behalf of the user to be performed before the user is identified.

FIA_UID.1.2/SC The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application note:

The GlobalPlatform TSF mediated actions listed in [GP] such as selecting an application, requestion data, initializing, etc.

FIA_UAU.1/SC Timing of authentication

FIA_UAU.1.1/SC The TSF shall allow **the TSF mediated actions listed in FIA_UID.1/SC** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2/SC The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.4/SC Single-use authentication mechanisms

FIA_UAU.4.1/SC The TSF shall prevent reuse of authentication data related to **the authentication mechanism used to open a secure communication channel with the card**.

5.1.2 SCWS TOE

The SFRs for the SCWS TOE configuration consist of all the SFRs for Basic TOE plus the following SFRs.

FPT_RPL.1/SCWS Replay detection

FPT_RPL.1.1/SCWS The TSF shall detect replay for the following entities:

- **http requests.**
- ***[assignment: list of identified entities]***.

FPT_RPL.1.2/SCWS The TSF shall perform **[assignment: list of specific actions]** when replay is detected.

FPT_FLS.1/SCWS Failure with preservation of secure state

FPT_FLS.1.1/SCWS The TSF shall preserve a secure state when the following types of failures occur: **[assignment: list of types of failures detected by the SCWS, including suspicious unauthenticated http requests]**.

Application note:

Sending multiple http requests to the SCWS without being authenticated is interpreted as a Denial Of Service attack on the SCWS.

FPT_TDC.1/SCWS Inter-TSF basic TSF data consistency

FPT_TDC.1.1/SCWS The TSF shall provide the capability to consistently interpret **HTTP(s) requests** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2/SCWS The TSF shall use

- **the rules defined in Sections 4 and 5 [HTTP/1.1] (for the MUST level requirements) for the interpretation of HTTP messages and requests.**
- **the rules defined in Section 13.1 of SCWS specification [SCWS] for the interpretation of administration commands**
- **[assignment: list of interpretation rules to be applied by the TSF]**

when interpreting the TSF data from another trusted IT product.

FTP_TRP.1/SCWS Trusted path

FTP_TRP.1.1/SCWS The TSF shall provide a communication path between itself and **remote** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **modification and disclosure**.

FTP_TRP.1.2/SCWS The TSF shall permit **remote users** to initiate communication via the trusted path.

FTP_TRP.1.3/SCWS The TSF shall require the use of the trusted path for **initial user authentication and**

- **SCWS administration**
- ***[assignment: other services for which trusted path is required]***.

Application note:

FTP_TRP.1.3/SCWS: SCWS administration comprise firewall data updates.

FTP_ITC.1/SCWS Inter-TSF trusted channel

FTP_ITC.1.1/SCWS The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2/SCWS The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

FTP_ITC.1.3/SCWS The TSF shall initiate communication via the trusted channel for

- **SCWS administration**
- ***[assignment: list of functions for which a trusted channel is required]***.

5.2 Security Assurance Requirements

The security assurance requirement level is EAL4 augmented with AVA_VAN.5 and ALC_DVS.2.

5.3 Security Requirements Rationale

5.3.1 Objectives

5.3.1.1 Security Objectives for the TOE

Basic TOE

Card Management

O.CARD-MANAGEMENT The security objective O.CARD-MANAGEMENT is met by the following SFRs:

- FDP_UIT.1/CCM enforces the Secure Channel Protocol information flow control policy and the Security Domain access control policy to ensure the integrity of card management operations.
- FDP_ROL.1/CCM ensures that card management operations may be cleanly aborted.
- FDP_ITC.2/CCM enforces the Firewall access control policy and the Secure Channel Protocol information flow policy when importing card management data.
- FPT_FLS.1/CCM preserves a secure state when failures occur.
- All SFRs related to Security Domains (FDP_ACC.1/SD, FDP_ACF.1/SD, FMT_MSA.1/SD, FMT_MSA.3/SD, FMT_SMF.1/SD, FMT_SMR.1/SD) cover this security objective by enforcing a Security Domain access control policy (rules and restrictions) that ensures a secure card content management.
- All SFRs related to the secure channel (FMT_MSA.1/SC, FMT_MSA.3/SC, FMT_SMF.1/SC, FIA_UAU.1/SC, FTP_ITC.1/SC, FCO_NRO.2/SC, FDP_IFC.2/SC, FDP_IFF.1/SC, FIA_UID.1/SC, FIA_UAU.4/SC) support this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.

O.DOMAIN-RIGHTS The security objective O.DOMAIN-RIGHTS is met by the following SFRs:

- All SFRs related to Security Domains (FDP_ACC.1/SD, FDP_ACF.1/SD, FMT_MSA.1/SD, FMT_MSA.3/SD, FMT_SMF.1/SD, FMT_SMR.1/SD) cover this security objective by enforcing a Security Domain access control policy (rules and restrictions) that ensures a secure card content management.
- All SFRs related to the secure channel (FMT_MSA.1/SC, FMT_MSA.3/SC, FMT_SMF.1/SC, FIA_UAU.1/SC, FTP_ITC.1/SC, FCO_NRO.2/SC, FDP_IFC.2/SC, FDP_IFF.1/SC, FIA_UID.1/SC, FIA_UAU.4/SC) support this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.

O.APPLI-AUTH The security objective O.APPLI-AUTH is met by the following SFRs:

- FDP_ROL.1/CCM ensures that card management operations may be cleanly aborted.
- FPT_FLS.1/CCM preserves a secure state when failures occur.
- FCS_COP.1/DAP ensures that the loaded Executable Application is legitimate by specifying the algorithm to be used in order to verify the DAP signature of the Verification Authority.

Communication

O.COMM_AUTH This security objective is covered by the following security functional requirements:

- FTP_ITC.1/SC which ensures the origin of card administration commands.
- FMT_SMR.1/SD specifies the authorized identified roles enabling to send and authenticate card management commands.
- FDP_IFC.2/SC and FDP_IFF.1/SC enforces the Secure Channel Protocol information flow control policy to ensure the origin of administration requests.
- FMT_MSA.1/SC and FMT_MSA.3/SC covers indirectly this security objective by specifying security attributes enabling to authenticate card management requests.
- FIA_UID.1/SC and FIA_UAU.1/SC specify the actions that can be performed before authenticating the origin of the APDU commands that the (U)SIM card receives.

The security functional requirement FCS_COP.1 defined in [JCRE] supports also this security objective by specifying secure cryptographic algorithm that shall be used to determine the origin of the card management commands.

O.COMM_INTEGRITY This security objective is covered by the following security functional requirements:

- FTP_ITC.1/SC which ensures the integrity of card management commands.
- FMT_SMF.1/SC specifies the actions activating the integrity check on the card management commands.
- FMT_SMR.1/SD defines the roles enabling to send and authenticate the card management requests for which the integrity has to be ensured.
- FDP_IFC.2/SC and FDP_IFF.1/SC enforces the Secure Channel Protocol information flow control policy to guarantee the integrity of administration requests.

- FMT_MSA.1/SC and FMT_MSA.3/SC covers indirectly this security objective by specifying security attributes enabling to guarantee the integrity of card management requests.

The security functional requirement FCS_COP.1 defined in [JCRE] supports also this security objective by specifying secure cryptographic algorithm that shall be used to ensure the integrity of the card management commands.

O.COMM_CONFIDENTIALITY This security objective is covered by the following security functional requirements:

- FTP_ITC.1/SC which ensures the confidentiality of card management commands.
- FMT_SMF.1/SC specifies the actions ensuring the confidentiality of the card management commands.
- FMT_SMR.1/SD defines the roles enabling to send and authenticate the card management requests for which the confidentiality has to be ensured.
- FDP_IFC.2/SC and FDP_IFF.1/SC enforces the Secure Channel Protocol information flow control policy to guarantee the confidentiality of administration requests.
- FMT_MSA.1/SC and FMT_MSA.3/SC covers indirectly this security objective by specifying security attributes enabling to guarantee the confidentiality of card management requests by decrypting those requests and imposing management conditions on that attributes.

The security functional requirement FCS_COP.1 defined in [JCRE] supports also this security objective by specifying secure cryptographic algorithm that shall be used to ensure the confidentiality of the card management commands.

SCWS TOE

O.INPUT-VALIDATION This security objective is covered by:

- FPT_TDC.1/SCWS which ensures a correct interpretation of HTTP(s) requests.
- FTP_ITC.1/SCWS which requires for administrative commands a secure channel that ensures the origin of the SCWS administration.
- FTP_TRP.1/SCWS which imposes for administrative commands a trusted path with the SCWS administrator when data is being updated.

O.DOS-DETECTION This security objective is covered by the security functionnal requirement FPT_FLS.1/SCWS which ensures that the TSF preserve a secure state even if there had been a Denial Of Service attack on the SCWS.

O.REPLAY This security objective is covered by the security functional requirement FPT_RPL.1/SCWS that ensures that http requests sent to the SCWS are protected from replay attacks. The TSF detects and reacts in rejecting those requests. It is also covered by the security functionnal requirement FTP_TRP.1/SCWS which provides assured identification of the two end points of the communication channel and protection of the communicated data from modification and disclosure.

5.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
O.CARD-MANAGEMENT	FDP_ACC.1/SD, FMT_MSA.1/SD, FMT_MSA.3/SD, FMT_SMF.1/SD, FMT_SMR.1/SD, FDP_UIT.1/CCM, FDP_ROL.1/CCM, FDP_ITC.2/CCM, FPT_FLS.1/CCM, FMT_MSA.1/SC, FMT_MSA.3/SC, FMT_SMF.1/SC, FIA_UAU.1/SC, FTP_ITC.1/SC, FCO_NRO.2/SC, FDP_IFC.2/SC, FDP_IFF.1/SC, FIA_UID.1/SC, FIA_UAU.4/SC, FDP_ACF.1/SD	Section 5.3.1
O.DOMAIN-RIGHTS	FDP_ACC.1/SD, FDP_ACF.1/SD, FMT_MSA.1/SD, FMT_MSA.3/SD, FMT_SMF.1/SD, FMT_SMR.1/SD, FMT_MSA.1/SC, FMT_MSA.3/SC, FMT_SMF.1/SC, FIA_UID.1/SC, FIA_UAU.1/SC, FIA_UAU.4/SC, FTP_ITC.1/SC, FCO_NRO.2/SC, FDP_IFC.2/SC, FDP_IFF.1/SC	Section 5.3.1
O.APPLI-AUTH	FDP_ROL.1/CCM, FPT_FLS.1/CCM, FCS_COP.1/DAP	Section 5.3.1
O.COMM_AUTH	FTP_ITC.1/SC, FMT_SMR.1/SD, FDP_IFC.2/SC, FDP_IFF.1/SC, FMT_MSA.1/SC, FMT_MSA.3/SC, FIA_UID.1/SC, FIA_UAU.1/SC	Section 5.3.1
O.COMM_INTEGRITY	FTP_ITC.1/SC, FMT_SMF.1/SC, FMT_SMR.1/SD, FDP_IFC.2/SC, FDP_IFF.1/SC, FMT_MSA.1/SC, FMT_MSA.3/SC	Section 5.3.1
O.COMM_CONFIDENTIALITY	FTP_ITC.1/SC, FMT_SMF.1/SC, FMT_SMR.1/SD, FDP_IFC.2/SC, FDP_IFF.1/SC, FMT_MSA.1/SC, FMT_MSA.3/SC	Section 5.3.1
O.INPUT-VALIDATION	FTP_TRP.1/SCWS, FTP_ITC.1/SCWS, FPT_TDC.1/SCWS	Section 5.3.1

Security Objectives	Security Functional Requirements	Rationale
O.DOS-DETECTION	FPT_FLS.1/SCWS	Section 5.3.1
O.REPLAY	FPT_RPL.1/SCWS, FTP_TRP.1/SCWS	Section 5.3.1

Table 7 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives
FDP_UIT.1/CCM	O.CARD-MANAGEMENT
FDP_ROL.1/CCM	O.CARD-MANAGEMENT, O.APPLI-AUTH
FDP_ITC.2/CCM	O.CARD-MANAGEMENT
FPT_FLS.1/CCM	O.CARD-MANAGEMENT, O.APPLI-AUTH
FCS_COP.1/DAP	O.APPLI-AUTH
FDP_ACC.1/SD	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS
FDP_ACF.1/SD	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS
FMT_MSA.1/SD	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS
FMT_MSA.3/SD	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS
FMT_SMF.1/SD	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS
FMT_SMR.1/SD	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM_AUTH, O.COMM_INTEGRITY, O.COMM_CONFIDENTIALITY
FTP_ITC.1/SC	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM_AUTH, O.COMM_INTEGRITY, O.COMM_CONFIDENTIALITY
FCO_NRO.2/SC	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS
FDP_IFC.2/SC	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM_AUTH, O.COMM_INTEGRITY, O.COMM_CONFIDENTIALITY
FDP_IFF.1/SC	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM_AUTH, O.COMM_INTEGRITY, O.COMM_CONFIDENTIALITY
FMT_MSA.1/SC	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM_AUTH, O.COMM_INTEGRITY, O.COMM_CONFIDENTIALITY
FMT_MSA.3/SC	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM_AUTH, O.COMM_INTEGRITY, O.COMM_CONFIDENTIALITY
FMT_SMF.1/SC	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM_INTEGRITY, O.COMM_CONFIDENTIALITY
FIA_UID.1/SC	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM_AUTH
FIA_UAU.1/SC	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS, O.COMM_AUTH
FIA_UAU.4/SC	O.CARD-MANAGEMENT, O.DOMAIN-RIGHTS
FPT_RPL.1/SCWS	O.REPLAY
FPT_FLS.1/SCWS	O.DOS-DETECTION

Security Functional Requirements	Security Objectives
FPT_TDC.1/SCWS	O.INPUT-VALIDATION
FTP_TRP.1/SCWS	O.INPUT-VALIDATION, O.REPLAY
FTP_ITC.1/SCWS	O.INPUT-VALIDATION

Table 8 SFRs and Security Objectives

5.3.3 Dependencies

5.3.3.1 SFRs dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FPT_RPL.1/SCWS	No dependencies	
FPT_FLS.1/SCWS	No dependencies	
FPT_TDC.1/SCWS	No dependencies	
FTP_TRP.1/SCWS	No dependencies	
FTP_ITC.1/SCWS	No dependencies	
FDP_UIT.1/CCM	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/SD, FTP_ITC.1/SC
FDP_ROL.1/CCM	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.1/SD
FDP_ITC.2/CCM	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/SD, FTP_ITC.1/SC
FPT_FLS.1/CCM	No dependencies	
FCS_COP.1/DAP	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.2/CCM
FDP_ACC.1/SD	(FDP_ACF.1)	FDP_ACF.1/SD
FDP_ACF.1/SD	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/SD, FMT_MSA.3/SD
FMT_MSA.1/SD	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/SD, FMT_SMF.1/SD, FMT_SMR.1/SD
FMT_MSA.3/SD	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/SD, FMT_SMR.1/SD
FMT_SMF.1/SD	No dependencies	
FMT_SMR.1/SD	(FIA_UID.1)	FIA_UID.1/SC
FTP_ITC.1/SC	No dependencies	
FCO_NRO.2/SC	(FIA_UID.1)	FIA_UID.1/SC
FDP_IFC.2/SC	(FDP_IFF.1)	FDP_IFF.1/SC
FDP_IFF.1/SC	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.2/SC, FMT_MSA.3/SC
FMT_MSA.1/SC	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/SD, FMT_SMR.1/SD, FMT_SMF.1/SC
FMT_MSA.3/SC	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1/SD, FMT_MSA.1/SC
FMT_SMF.1/SC	No dependencies	

Requirements	CC Dependencies	Satisfied Dependencies
FIA_UID.1/SC	No dependencies	
FIA_UAU.1/SC	(FIA_UID.1)	FIA_UID.1/SC
FIA_UAU.4/SC	No dependencies	

Table 9 SFRs dependencies

5.3.3.2 SARs dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.4, ADV_TDS.3
ADV_FSP.4	(ADV_TDS.1)	ADV_TDS.3
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.3, ALC_TAT.1
ADV_TDS.3	(ADV_FSP.4)	ADV_FSP.4
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	No dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4, ALC_DVS.2, ALC_LCD.1
ALC_CMS.4	No dependencies	
ALC_DEL.1	No dependencies	
ALC_DVS.2	No dependencies	
ALC_LCD.1	No dependencies	
ALC_TAT.1	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No dependencies	
ASE_INT.1	No dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.4, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.4, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) and (ADV_TDS.2) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.3, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1

Table 10 SARs dependencies

5.3.4 Rationale for the Security Assurance Requirements

EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It corresponds to a white box analysis and it can be considered as a reasonable level that can be applied to an existing product line without undue expense and complexity.

The TOE is intended to operate in open environments, where attackers can easily exploit vulnerabilities. According to the claimed intended usage of the TOE, it is very likely that it may represent a significant value and then constitute an attractive target for attacks. In some malicious usages of the TOE the statistical or probabilistic mechanisms in the TOE, for instance, may be subjected to analysis and attack in the normal course of operation. An EAL 4 augmented with ALC_DVS.2 and AVA_VAN.5 seems to be the reasonable minimum level for (U) SIM cards hosting sensitive applications. It shall probably be the case, as it is frequent nowadays, that the required evaluation assurance level will be high in, for instance, banking or electronic signature applications.

5.3.5 AVA_VAN.5 Advanced methodical vulnerability analysis

This component added to EAL 4 package in order to provide sufficient robustness to counter an attacker with high attack potential without the support of a protecting environment. Moreover, the (U)SIM card is a generic platform that could be used for a wide range of applications, including highly sensitive ones, like identity cards, pay-TV, e-cards, or credit cards. Potential attackers for such kind of applications include international organizations, or even a state, disposing of important means and resources.

5.3.6 ALC_DVS.2 Sufficiency of security measures

This component was added in order to provide a higher assurance on the security of the (U)SIM cards development and manufacturing processes, especially for the secure handling of the embedded software and data. Those requirements appear as the most adequate ones for a manufacturing process in which several actors (Platform Developer, Operator, Application Developers, IC Manufacturer, etc) exchange and store highly sensitive information (confidential code, cryptographic keys, personalisation data, etc).

Annexe A Definitions and Acronyms

A.1 Definitions

This section provides definitions about terms frequently used in this document. The definition of the Common Criteria related terms is specified in [CC1], § 4.

ITSEF	IT Security evaluation laboratory approved by the certification body of the country where the evaluation is performed. It manages Common Criteria evaluations of platforms and secure applications.
(U)SIM Java Card Platform developer	Company which manages the development of the (U)SIM Java Card Platform.
Application developer	Company which develops secure or standard applications that shall be loaded onto the platform.
Application provider	Entity or organization which manages the application and the associated services. It can be a bank, a transport operator or a third-party service provider.
Certification body	State office which manages the Common Criteria certification of the platforms and the secure applications evaluated by an ITSEF. In France, it is the ANSSI.
Issuer	See TOE issuer.
Mobile operator	Owner of the (U)SIM Java Card Platform which also manages a mobile network.
Smart Card IC Provider	Company which manages the development and the production of the IC.
Smart Card manufacturer	Company which manages the manufacturing of the (U)SIM card, especially in the IC Card manufacturing phase product.
Smart Card personalizer	Company which performs the personalization of the (U)SIM Java Card Platform.
TOE issuer	See mobile operator.
Verification Authority	Trusted entity which signs application after validation or certification. The application signature is verified on the card at loading by an agent of the VA which is present on the platform.
Validation laboratory	Accredited Security laboratory approved by the Mobile Operator which manages the validation of the standard applications.
Controlling Authority	Entity represented on the (U)SIM card responsible for securing the keys creation and personalisation of the Application Provider Security Domain (APSD).

A.2 Acronyms

3GPP	3rd Generation Partnership Project
ACP	Access Control Policy
ADELG	Applet Deletion Group
AID	Applet IDentifier
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
AP	Application Provider
APDU	Application Protocol Data Unit
API	Application Programming Interface
APSD	Application Provider Security Domain
BIP	Bearer Independent Protocol
CA	Controlling Authority
CAD	Card Acceptance Device
CASD	Controlling Authority Security Domain
CC	Common Criteria
CEM	Common Evaluation Methodology
EAL	Evaluation Assurance Level
EMV	EuroPay, MasterCard, Visa
ETR_COMP	Report for a composite Smart Card Evaluation
GSM	Global System for Mobile communications
HSP	High Speed Protocol
HW/SW/FW	Hardware/Software/Firmware
IC	Integrated Circuit
IMSI	International Mobile Subscriber Identity
ISCI	International Security Certification Initiative
ITSEF	Information Technology Security Evaluation Facility
JCRE	Java Card Runtime Environment
JCS	Java Card System
JCVM	Java Card Virtual Machine
LCG	Logical Channel Group
MNO	Mobile Network Operator
NFC	Near Field Communication

3GPP	3rd Generation Partnership Project
OS	Operating system
OSP	Organizational Security Policy
PDA	Personal Digital Assistant
PP	Protection Profile
RMI	Remote Method Invocation
SCP	Smart Card Platform
SCWS	Smart Card Web Server
SF	Security Function
SIM	Subscriber Identity Module
SPD	Security Problem Definition
SSCD	Secure Signature Creation Device
ST	Security Target
SWP	Single Wire Protocol
TOE	Target Of Evaluation
TSF	TOE Security Functions
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
USAT	USIM Application Toolkit
USB	Universal Serial Bus
USIM	Universal Subscriber Identity Module
VA	Verification Authority

Annexe B References

[CC1]	CCMB, *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1 - Revision 3*, July 2009, CCMB-2009-07-001.
[CC2]	CCMB, *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements*, Version 3.1 - Revision 3, July 2009, CCMB-2009-07-002.
[CC3]	CCMB, *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements*, Version 3.1 - Revision 3, July 2009, CCMB-2009-07-003.
[CEM]	CCMB, *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, Version 3.1 – Revision 3, July 2009, CEM-2009-07-004.
[Comp]	CCDB, *Composite product evaluation for Smart Cards and similar devices*, September 2007, Version 1.0 - Revision 1, September 2007, CCDB-2007-09-001
[GP]	GlobalPlatform, *Card Specification*, Version 2.2, March 2006
[GP-CCCM]	GlobalPlatform, *Card Confidential Card Content Management, Card specification v2.2 – Amendment A*, Version 1.0, October 2007
[GP-UICC]	GlobalPlatform, *Card UICC Configuration*, Version 1.0, October 2008
[JCAPI]	Sun Microsystems, Inc., *Java Card Platform, version 2.2.2 Application Programming Interface*, March 2006. Sun Microsystems, Inc., *Java Card Platform, version 3.0, Classic Edition, Application Programming Interface*, March 2008.
[JCRE]	Sun Microsystems, Inc., *Java Card Platform, version 2.2.2 Runtime Environment (Java Card RE) Specification*, March 2006. Sun Microsystems, Inc., *Java Card Platform, version 3.0, Classic Edition, Runtime Environment (Java Card RE) Specification*, March 2008.
[JCVM]	Sun Microsystems, Inc., *Java Card Platform, version 2.2.2 Virtual Machine (Java Card VM) Specification*, October 2005. Sun Microsystems, Inc., *Java Card Platform, version 3.0, Classic Edition, Virtual Machine (Java Card VM) Specification*, March 2008.
[HTTP/1.1]	*Hypertext Transfer Protocol -- HTTP/1.1*, RFC 2616, June 1999.
[Platform]	Trusted Labs, *Exigences sur les plateformes SIM/USIM*, CP-2007-RT-415-2.0.
[PP0902]	*Embedded Software for Smart Secure Devices Protection Profile*, Version 1.0, November 2009, ANSSI-CC-PP-2009/02.
[PP SSCD-BSI-0005-2002]	CEN/ISSS, *Protection Profile — Secure Signature Creation Device Protection Profile (SSCD)*, 2002, PP SSCD-BSI-0004-2002 type 1, PP SSCD-BSI-0005-2002 type 2, PP SSCD-BSI-0005-2002 type 3
[PP-JCS]	Sun Microsystems, Inc., *Java Card System Open Configuration Protection Profile*, April 2010, ANSSI-CC-PP-2010/03.

[CC1]	CCMB, *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1 - Revision 3*, July 2009, CCMB-2009-07-001.
[PP0035]	Eurosmart, *Security IC Platform Protection Profile*, Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035.
[SCWS]	OMA, *Smartcard Web Server*, Approved Version 1.1, 12 May 2009.
[Secure APP]	Trusted Labs, *Guide de composition CC entre plateformes certifiées et applications* sensibles, CP-2007-RT-407-3.0
[Basic APP]	Trusted Labs, *Règles pour les applications non sensibles*, CP-2007-RT-454-2.0
[TS03.19]	ETSI 3GPP TS 03.19, *Subscriber Identity Module Application Programming Interface (SIM API) for Java Card™; Stage 2 (Release 1999)*
[TS102.241]	ETSI TS 102.241, *Smart Cards; UICC Application Programming Interface (UICC API) for Java Card™ (Release 6)*
[T131.130]	ETSI TS 131.130, *Digital cellular telecommunications system (Phase 2+);Universal Mobile Telecommunications System (UMTS);(U)SIM Application Programming Interface (API);(U)SIM API for Java Card (3GPP TS 31.130 version 6.6.0 Release 6)*
[TS102.223]	ETSI 3GPP TS 102.223, *Smart Cards; Card Application Toolkit (CAT) (Release 6)*
[TS102.225]	ETSI 3GPP TS 102.225, *Smart Cards ; Secured packet structure for UICC based applications (Release 6)*
[TS102.226]	ETSI 3GPP TS 102.226, *Smart Cards; Remote APDU structure for UICC based applications (Release 6)*
[TS102.613]	ETSI 3GPP TS 102.613, *Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics (Release 7)*
[TS102.622]	ETSI 3GPP TS 102.622, *Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI) (Release 7)*
[TS131.111]	ETSI 3GPP TS 131.111, *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Universal Subscriber Identity Module (USIM) Application Toolkit (USAT) (Release 6)*

Index

This document has been generated with TL SET version 2.3.6 (for CC3). For more information about the security editor tool of Trusted Labs visit our website at www.trusted-labs.com.

End of document