

ST4SIM-201

Security Target

Version: 1.3
Date: 2022-05-16
STMicroelectronics

Document history

Version	Date	Comment	Author
0.4	2021-10-25	Shared with STMicroelectronics	SGS Brightsight
0.5	2021-11-09	Update STMicroelectronics	SGS Brightsight
0.6	2021-12-17	Initial draft version	SGS Brightsight
0.7	2022-02-03	Update to Java Card 3.0.5 PP and readability improvements	SGS Brightsight
0.7.1	2022-02-14	Fixed chip version	STMicroelectronics
0.7.2	2022-02-14	Fixed TOE name	SGS Brightsight
0.8	2022-03-04	Update ASE findings	SGS Brightsight
1.0	2022-04-19	Candidate version	STMicroelectronics SGS Brightsight
1.1	2022-05-02	Updated TOE delivery definition	STMicroelectronics
1.2	2022-05-12	Updated TOE delivery procedure	STMicroelectronics
1.3	2022-05-16	Updated TOE delivery procedure	STMicroelectronics

Distribution list

- STMicroelectronics
- GSMA/TrustCB
- SGS Brightsight

Contents

1	ST Introduction	6
1.1	ST Reference	6
1.2	TOE Reference	6
1.2.1	Other certifications	6
1.3	TOE Overview	6
1.4	TOE Description	7
1.4.1	TOE Definition	7
1.4.1.1	Profile interpreter	8
1.4.1.2	Telecom framework	8
1.4.1.3	Notification / Profile switch / Fallback	8
1.4.1.4	Platform layer	9
1.4.2	TOE Usage and Major Security Features	10
1.4.3	Logical scope	10
1.4.3.1	Remote SIM provisioning	11
1.4.3.2	Test profile support	11
1.4.3.3	Supported algorithms	11
1.4.3.4	Over the air	12
1.4.3.5	Java Card	12
1.4.3.6	Memory management	12
1.4.3.7	Extensible Authentication Protocol (EAP)	13
1.4.3.8	Cryptography	13
1.4.3.9	UICC ETSI Suspension and Poll Interval Negotiation	13
1.4.4	Non-TOE Hardware/Software/Firmware	13
1.4.5	TOE Life Cycle	15
2	Conformance claims	16
2.1	CC Conformance Claims	16
2.2	Package Claims	16
2.3	PP Claims	16
2.4	Conformance Rationale	16
2.4.1	Security Problem Definition Statement	16
2.4.2	Security Objectives Statement	16
2.4.2.1	Java Card	16
2.4.2.2	eUICC	17
2.4.3	Security Functional Requirements Statement	18
2.4.3.1	Java Card	18
2.4.3.2	eUICC	18
3	Security Problem Definition	19
3.1	Java Card	19
3.2	eUICC	19
4	Security Objectives	20
4.1	JavaCard	20
4.1.1	Security Objectives for the TOE	20

4.1.2	Security Objectives for the Operational Environment.....	21
4.1.3	Security Objectives Rationale	21
4.2	eUICC	21
4.2.1	Security Objectives for the TOE.....	21
4.2.2	Security Objectives for the Operational Environment.....	21
4.2.3	Security Objectives Rationale	21
5	Extended Component Definition	22
5.1	eUICC	22
5.2	Java Card.....	22
6	Security Functional Requirements	23
6.1	Java Card.....	23
6.1.1	COREG_LC SECURITY FUNCTIONAL REQUIREMENTS.....	23
6.1.1.1	Firewall policy.....	24
6.1.1.2	Application Programming Interface.....	24
6.1.1.3	Card Security Management	27
6.1.1.4	AID Management	29
6.1.2	InstG Security Functional Requirements	31
6.1.2.1	FPT_RCV.3/Installer Automated recovery without undue loss.....	31
6.1.3	ADELG Security Functional Requirements.....	32
6.1.4	ODELG Security Functional Requirements	32
6.1.5	CarG Security Functional Requirements	33
6.1.5.1	FCO_NRO.2/CM Enforced proof of origin	33
6.1.5.2	FDP_IFF.1/CM Simple security attributes	33
6.1.5.3	FDP_UIT.1/CM Data exchange integrity	34
6.1.5.4	FIA_UID.1/CM Timing of identification.....	35
6.1.5.5	FMT_MSA.1/CM Management of security attributes.....	35
6.1.5.6	FMT_MSA.3/CM Static attribute initialisation	35
6.1.5.7	FMT_SMF.1/CM Specification of Management Functions	35
6.1.5.8	FMT_SMR.1/CM Security roles	36
6.2	eUICC	37
6.2.1	Identification and authentication	38
6.2.1.1	FIA_UID.1/EXT Timing of identification	38
6.2.1.2	FIA_UAU.1/EXT Timing of authentication	38
6.2.2	Communication	39
6.2.2.1	FDP_IFF.1/SCP Simple security attributes.....	39
6.2.2.2	FTP_ITC.1/SCP Inter-TSF trusted channel.....	39
6.2.2.3	FDP_ITC.2/SCP Import of user data with security attributes	41
6.2.2.4	FPT_TDC.1/SCP Inter-TSF basic TSF data consistency.....	41
6.2.2.5	FCS_CKM.2/SCP-MNO Cryptographic key distribution	42
6.2.2.6	FCS_CKM.4/SCP-SM Cryptographic key destruction.....	43
6.2.2.7	FCS_CKM.4/SCP-MNO Cryptographic key destruction.....	43
6.2.3	Security Domains	44
6.2.3.1	FDP_ACF.1/ISDR Security attribute based access control.....	44
6.2.3.2	FDP_ACF.1/ISDP Security attribute based access control	46
6.2.4	Platform Services	47

6.2.4.1	FDP_IFF.1/Platform_services Simple security attributes	48
6.2.4.2	FPT_FLS.1/Platform_Services Failure with preservation of secure state	48
6.2.5	Security management	49
6.2.5.1	FCS_RNG.1 Random number generation	49
6.2.5.2	FCS_COP.1/DRBG Cryptographic Operation	50
6.2.5.3	FPT_EMS.1 TOE Emanation	50
6.2.5.4	FMT_SMF.1/EUICC Specification of Management Functions	51
6.2.6	Mobile Network authentication	51
6.2.6.1	FCS_COP.1/Mobile_network Cryptographic operation	51
6.2.6.2	FCS_CKM.2/Mobile_network Cryptographic key distribution	51
6.2.6.3	FCS_CKM.4/Mobile_network Cryptographic key destruction	52
7	Security Assurance Requirements	53
8	TOE Summary Specification	54
8.1	Security Functionality	54
8.1.1	Java Card	54
8.1.2	eUICC	56
9	Rationales	58
9.1	Security Requirements Rationale	58
9.1.1	Java Card	58
9.1.1.1	Objectives	58
9.1.1.2	Rationale tables of Security Objectives and SFRs	61
9.1.1.3	Dependencies	62
9.1.1.4	SFR Dependencies	62
9.1.1.5	SARs Dependency Rationale	64
9.1.2	eUICC	66
9.1.2.1	Objectives	66
9.1.2.2	Rationale tables of Security Objectives and SFRs	67
9.1.2.3	Dependencies	68
9.1.2.4	SFR Dependencies	68
9.1.2.5	SARs Dependency Rationale	70
9.2	IC Composition rationale	72
9.2.1	Common Criteria rationale	72
9.2.2	Compatibility between threats (TOE and IC)	72
9.2.3	Compatibility between assumptions (TOE and IC)	72
9.2.4	Compatibility between security objectives for the environment (TOE and IC)	73
9.2.5	Compatibility between Security Objectives (TOE and IC)	73
9.2.6	Compatibility between Organisational Security Policies (TOE and IC)	73
9.2.7	Compatibility between SFRs (TOE and IC)	74
10	Abbreviations and glossary	76
11	References	77

1 ST Introduction

This section provides information about the TOE, which enables a potential user of the TOE to determine, whether the TOE implements the functionality required by the user.

1.1 ST Reference

Title	ST4SIM-201 Security Target
Version	See Document History
Date	See Document History
Author	STMicroelectronics

Table 1 Security Target reference

1.2 TOE Reference

TOE Name	ST4SIM201	
TOE Version	v1.0.8	
TOE Identification	IC Java Card OS and eUICC functionality	IC Name: ST33G1M2M / ST33G1M2A IC Maskset name: K8H0A Version: G Master product identification number: 0x00F3 (ST33G1M2M) / 0x00F2 (ST33G1M2A) Firmware version: 1.3.2 OST version: 2.2 Neslib crypto library version : 6.3.4 OS_IDENTIFIER: 0x0000 OS_RELEASE_DATE: 0x2090 OS_RELEASE_LEVEL: 0x0001 OS_VERSION: 0x00010008
TOE Type	UICC embedded in a machine-to-machine Device	

Table 2 TOE reference

1.2.1 Other certifications

The ST33G1M2M/A C01 Secure IC has been already certified:

- IC name: ST33G1M2M and ST33G1M2A C01 platform
- CC certificate reference [CERT-IC].

1.3 TOE Overview

The TOE consists of the following components:

- Secure IC including a kernel with memory management, ISO7816 communication protocol, memory manager and Cryptographic operation based on the NesLib security library.
- Java Card runtime environment supporting multiple profiles.
- Telecom framework
- Application layer including ISDP, ISDR and eCASD.

An overview of the TOE scope taken from [PP-eUICC] is shown in Figure 1

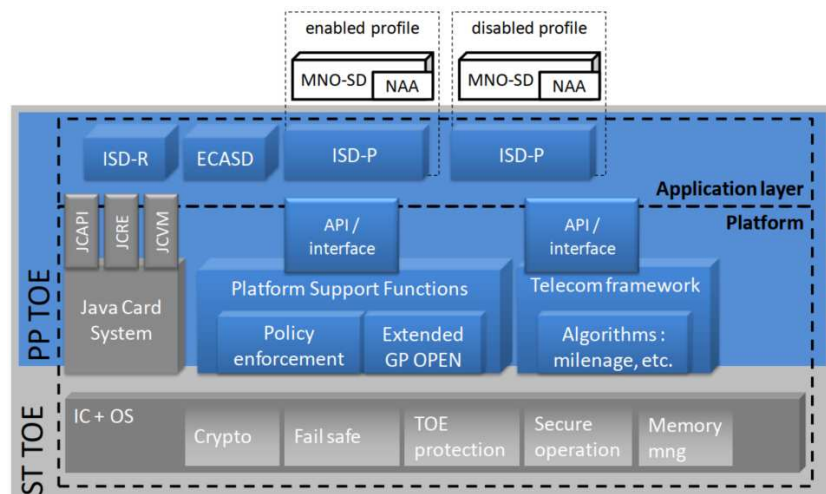


Figure 1 Scope of the TOE

1.4 TOE Description

1.4.1 TOE Definition

The TOE is a eUICC is an UICC embedded in a machine-to-machine Device and connected to a given mobile network, by the means of its currently enabled MNO Profile.

The TOE is a composite TOE comprising hardware and software. The physical scope is defined as:

- the STMicroelectronics IC ST33G1M2M/A Security Integrated Circuit with dedicated software and embedded cryptographic library. Common criteria certified by ANSSI with assurance level EAL5+ [CERT-IC].
- An encrypted image of the ST4SIM-201 Operating system, including:
 - the Java Card Operating System version 3.0.5.
 - the embedded UICC implementation that supports the USIM applications providing access to Universal Mobile Telecommunications System (UMTS) networks and the IP Multimedia Services Identity Module (ISIM) to access IP Multimedia Subsystem (IMS) networks.
- the associated guidance documentation in printed copy delivered in .pdf format delivered encrypted by e-mail:
 - Operational User Guidance Rev. H
 - Preparative Procedure Rev. H

The encrypted image of the ST4SIM-201 OS is transferred to STMicroelectronics engineering department encrypted via PGP by using shared repositories.

The TOE is delivered by a trusted courier at the end of the phase b (see Section 1.4.5).

The following form factors shall be supported:

- VDFFPN 8-pin very thin fine pitch dual flat package no lead - 5 mm × 6 mm, 1.27 mm pitch, with wettable flank. (for ETSI MFF2)
- TSSOP 20-lead thin shrink small outline package - body 4.4 mm pitch 0.65 mm.
- D16 micromodule (for ETSI 2FF/3FF/4FF)
- WLCSP11, 11-ball wafer-level chip-scale package available for the ST33G1M2M only.

Figure 2 shows the high level architecture of the TOE.

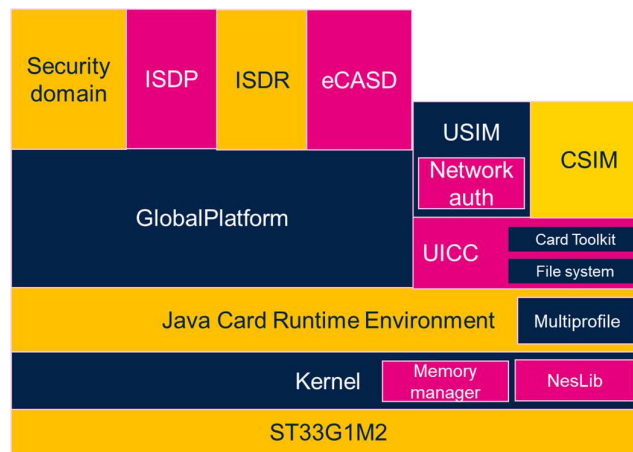


Figure 2 TOE Architecture

1.4.1.1 Profile interpreter

Profile interpreter executes the command decrypted by the ISD-P (SCP03t); DER coding is seen as a sequence of TLV that are then dispatched to the profile elements. Once this is performed, the operations are mapped over the corresponding administrative commands, e.g. the applet loading is mapped on GlobalPlatform commands, the file creation over file administration commands, etc. Sensitive data (like PIN, Keys, authentication credentials...) are masked by random masks.

1.4.1.2 Telecom framework

The Telecom framework has three main impacts on the RSP functionalities:

- File system management – multiple MF are defined as root of the several file structures for the profiles
- Card Toolkit protocols – SCP80 and SCP81 are based on card toolkit specification; SCP80 and SCP81 contribute to the security of the RSP; nevertheless, for most sensitive operations, SCP03t and confidential personalization protocols are enforced over SCP80 / SCP81.
- Authentication algorithms – the algorithms Milenage, Tuak and Test are supported.

1.4.1.3 Notification / Profile switch / Fallback

The procedure of profile change in SGP.02 v4.2 requires that, at profile change time, the eUICC shall:

- Require a RESET by issuing the REFRESH proactive command
- Change the current enabled profile
- Verify the coverage of the new profile
- Notify the server that the change has occurred
- Get a notification confirmation by the server

The procedure leaves many options to configurability and interpretation; hence such a functionality is provided in our product by a java card applet that is customizable for customers.

Similarly, the Fallback application manages explicit requests by external entities (like the modem) to switch to the fallback profile.

1.4.1.4 Platform layer

1.4.1.4.1 IC+OS

The hardware is ST33G1M2M/A, secure chip based on SC300 core. On the IC the Kernel executes that manages physical / communication protocol (ISO7816), memory manager and Cryptographic operation.

Crypto operations are mainly based on security library.

Mask of personalized data is differentiated chip by chip (ie. it is randomized during production).

In addition, an anti-tear mechanism is present that allows integrity of operation and transactions also in case of power loss.

1.4.1.4.2 Java card system

The Java Card contains the registry of the profiles and the profile status (like which is the fallback profile, which is the currently enabled profile, etc.).

Applications architecture is based on Java Card, also for Security Domains and network access applications (like USIM or CSIM); such system applications access to the product OS resources by using specific “native” methods, ie. methods that allow the execution directly in “C” code.

The virtual machine keeps track of the current profile that can be seen as the profile of the applet currently in execution.

1.4.1.4.3 GlobalPlatform

The GlobalPlatform manages all the card content management operations and it has been extended to support the multi-profile operation.

In particular:

- The ISD-R has been introduced as an extension of the Security Domain; the ISD-R contains SCP80 and SCP81 credentials that are used to perform SGP.02 operations.

In addition, it is the only entity that can install / enable / disable / delete ISD-Ps.

Other ISD-R functionalities (Notification and requests for profile rollback) are performed with the support of an additional application (NotificationManager) that is subject to customization for specific products.

The ISD-R is also in charge of enforcing the policy rules of the profiles.

- The ISD-P is the container of the profile, it is installed by the ISD-R and personalized through the eCASD. The ISD-P contains a SCP03t keyset (typically but not necessarily established through the eCASD) and receives, encrypted via the SCP03t, the profile package. A sub module of the ISD-P is the profile package interpreter, that execute the ASN.1 format.

The ISD-P can be installed and personalized over the SCP81 or SCP80 protocols; nevertheless, profile download in SCP03t may occur only over the SCP81 protocol.

The MNO-SD belongs to a profile and it represents the “Issuer security domain” of the currently enabled profile; it does not have all the privileges of the ISD as it cannot lock the card or perform other operations that have impact beyond the operator profile.

1.4.2 TOE Usage and Major Security Features

The TOE integrates a new secure architecture and complete ecosystem able to manage cellular network connectivity remotely without impacting the eSIM component.

Thanks to this eSIM technology, IoT devices can now be deployed to the field with one network connectivity solution and if at some later stage, this solution needs to be changed, a new one can be put in place through the network. So, no need for a product recall, nor product maintenance.

This solution is flexible and does not depend on a particular operator. For M2M, including industrial and automotive markets, this solution is service-oriented; the profile is remotely controlled by the service provider through a platform (push model). In this case, end-user interaction is not required.

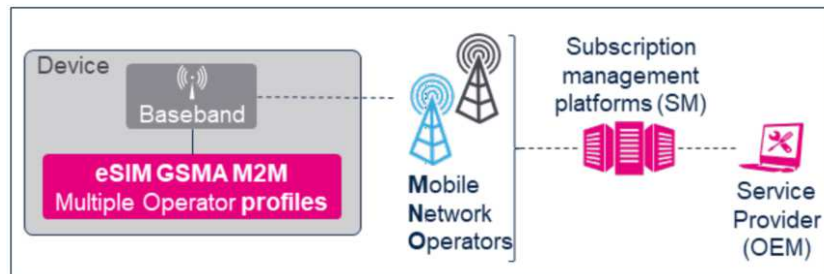


Figure 3 TOE usage scenario.

The ST4SIM-201 integrates the GSMA architecture with the profile management mechanisms. A profile contains the operator network data related to a subscription (operator's credentials, file system, PINs/PUKs, network authentication, application and so on). Each profile is independent of other profiles.

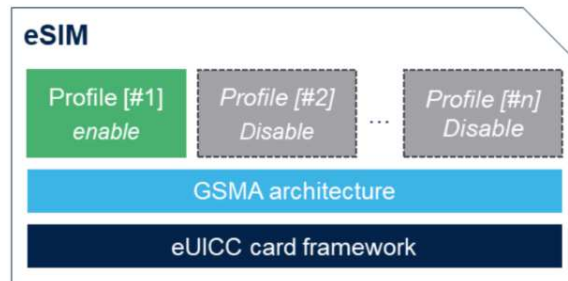


Figure 4 TOE usage scenario.

The ST4SIM-201 can host up to 7 profiles. Each profile has sufficient memory size available in the device or can have a specific memory size coded using the cumulative granted memory defined by GlobalPlatform amendment C [GP-C].

1.4.3 Logical scope

The ST4SIM-201 is a top-class multi-application Java Card™ platform, developed on top of a performing hardware architecture based on a powerful ARM® SecurCore® SC300™ 32-bit RISC core.

The Java Card based operating system complies with the ETSI and 3GPP Rel-16 specifications. The ST4SIM-201 supports the USIM applications providing access to Universal Mobile Telecommunications System (UMTS) networks and the IP Multimedia Services Identity Module (ISIM) to access IP Multimedia Subsystem (IMS) networks.

By supporting the ISIM, the ST4SIM-201 eUICC helps to improve the convergence of mobile, landline and full IP networks, exploiting all the capabilities of the Internet in a full packet switched based network.

The ST4SIM-201 supports the Java Card 3.0.5 classic API, as well as the ETSI, 3GPP UICC and USIM application programming interface (API).

The ST4SIM-201 platform is completed by a remote applet management fully integrated with GlobalPlatform card specification v.2.3, and also includes Amendment A [GP-A] (Confidential card content management), RAM over HTTP according to GP 2.3 Amendment B [GP-B], SCP03 protocol according to Amendment D [GP-D], Card content management updated to Elliptic Curve Cryptography according to Amendment E [GP-E].

The card also supports the ETSI standard administrative commands according to [TS 102 222] and a Dynamic Memory Management integrated with Java Card garbage collection mechanism.

1.4.3.1 Remote SIM provisioning

The ST4SIM-201 platform supports all the mechanisms defined by the GSMA SGP.02 v4.2 specifications to perform ISD-R, ISD-P and profile management. It fully implements the ES5 interface (SM-SR/eUICC), ES8 (SM-DP/eUICC), ES6 (MNO/eUICC). Based on GSMA defined certificates, ISD-P personalization is based on GlobalPlatform Amendment E [GP-E] key agreement, but it is also possible to configure ISD-P by using PUT KEY command allowing unbound protection of profiles.

The ST4SIM-201 platform fully supports SIMalliance interoperable profile package v2.3.1. No proprietary features are introduced. Profiles are coded according to ASN.1/DER coding and can be downloaded by using SCP03t over HTTPs (download via CAT-TP is not supported).

The card may host up to 7 profiles; every profile may have a specific memory quota coded according to GlobalPlatform Amendment C [GP-C] for non-volatile memory or use up to the card available memory for its purpose. Each profile contains a full file system structure (MF, ADFs, ...) with its own PINs/PUKs, NAA authentication information, etc. plus an MNO-SD and additional Security Domains.

Each profile is independent from the other profiles, i.e. it is possible to have in two profiles an application with the same AID, TAR or global service.

In addition, on the card there is a basic profile (defined as profile 0) that contains ISD-R, ISD and eCASD, that are visible whatever is the selected profile. It is possible to store in the profile 0 other applications; in this case, such applications shall be visible whatever the selected profile is. Also java card library packages can be stored in profile 0; all the card provided library packages (java card, sim toolkit, etc.) belong to the profile 0.

1.4.3.2 Test profile support

In addition to Remote SIM provisioning, test profiles can be loaded before issuance. Such profiles shall be available for local and remote profile switch to allow device integrator to test with network simulator equipment.

The local profile switch can be configured to be executed over the ISO interface.

The test profile feature can be disabled before issuance or after issuance with proper credentials.

1.4.3.3 Supported algorithms

The ST4SIM-201 platform supports all the standard authentication algorithms: CAVE and XOR, as well as the 3G-Milenage authentication algorithm.

In particular, the Milenage 3G algorithm enables authorized access to UMTS/LTE networks with an easy and flexible parameter customization, according to specific MNO requirements. In eUICC CAVE and XOR, as well as the 3G-Milenage authentication algorithm, also the TUAK algorithm has been introduced in both 128 and 256 variants.

In order to increase security performance, the ST4SIM-201 incorporates a ratification counter that limits the number of authentications attempts up to a MAX_VALUE defined by the MNO. This countermeasure is

available to prevent brute-force attacks from breaking algorithms. In addition, all the algorithms support dedicated countermeasures for DPA/SPA attacks.

1.4.3.4 Over the air

The ST4SIM-201 supports the ETSI standard Over the Air (OTA) protocol for Remote Applet Management (RAM) and Remote File Management (RFM) in compliance with ETSI TS 102 225 and ETSI TS 102 226 specifications Release 16.

The RAM (Remote Applet Management) application is also fully supported and integrated with Global Platform 2.3 and the related Amendment B [GP-B] (allowing the possibility to perform Remote Applet Management and Remote File Management over HTTP/TLS). TLS is available according to versions 1.0, 1.1 and 1.2; in addition, a proprietary mechanism allows the card to request a DNS server the HTTPs server address.

With the ST4SIM-201 it is possible to remotely control over-the-air the execution of APDU commands to administrate the card contents and of proactive commands to interact with the host handset; the ST4SIM-201 supports the secured packet structure and the remote APDU structure for (U)SIM Toolkit applications, according to 3GPP TS 31.115 and 31.116 specifications.

CAT-TP according to ETSI release 7 is supported; configuration of CAT-TP and related memory allocation (for PDUs, SDUs, etc.) is performed at card configuration and it applies to all profiles. RAM/RFM over IP is also supported.

As it is compliant with the ETSI, 3GPP and 3GPP2, the ST4SIM-201 family can be easily and effortlessly integrated into any OTA platform compliant with relevant standards. STMicroelectronics cards are field-proven to be interoperable with the mainstream OTA platforms commonly chosen by mobile network operators.

1.4.3.5 Java Card

ST4SIM-201 supports Java Card v3.0.5 classic edition; all the mandatory features are included, plus in addition support of int type and of object deletion.

1.4.3.6 Memory management

The OTA mechanism is completed by the support of 3G UICC Administrative Commands as specified by ETSI [TS 102 222]; these commands are integrated by a powerful dynamic memory management that allows complete smart memory defragmentation. As these commands are purely administrative, no security is claimed.

The standard commands contemplated in the above mentioned specification can thus be used to create or delete files with immediate memory reclaim.

Dynamic Memory Management provides:

- Common space for files/packages/applets/objects
- Memory recovery on deletion operations
- Total free memory available in the Select MF response.

The mechanism is designed to allow a very fast and silent memory recovery, absolutely safe for the end user data.

ST4SIM-201 is capable of enhancing intrinsic flash memory cells for those files which require intense update and higher reliability.

Memory quota mechanism based on the GlobalPlatform Amendment C [GP-C] (CGM) is supported; the mechanism can be disabled at card configuration.

Volatile memory management is based on an ST patented mechanism that optimizes the available resources for the enabled profile while guaranteeing resources for the downloading profile and the disabled profiles.

1.4.3.7 Extensible Authentication Protocol (EAP)

The ST4SIM-201 also supports the Extensible Authentication Protocol Method for GSM Subscriber Identity, or EAP-SIM, and the Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement, or EAP-AKA.

The Extensible Authentication Protocol (EAP) is a framework that provides a standard mechanism for authentication to access Wireless LAN: it allows for authentication and session key distribution using a GSM SIM cards (EAP-SIM) or a 3G USIM card (EAP-AKA) allowing users to login, for example, to a Wireless LAN.

By inserting the ST4SIM-201 in a PC or in a mobile phone supporting 802.1X wireless LAN client software, the supplicant (the UICC and Mobile/PC) communicates with the 802.1x hotspot access point and the Radius server identifying the end user via the challenge/secret response through his MNO HLR. The ST4SIM-201 eUICC implementation is the suitable means to grant the end user network access whenever he comes across any WiFi hotspots.

No security functionality is claimed for the EAP.

1.4.3.8 Cryptography

Besides standard symmetric cryptography and hashing algorithms (DES, TDES, AES, MD5, ...) the ST4SIM-201 family provides a crypto co-processor with up to 2048 bit long keys asymmetric cryptography capabilities such as RSA or Elliptic Curve Cryptography (ECC) up to 521 bit, for applications demanding the strongest level of cryptography.

The ST4SIM-201 fully supports the PKCS#15 standard and offers a rule-based access control mechanism such as digital signature/certificates for data/applications requiring a strong level of cryptography.

The ST4SIM-201 implement javacard.security as well as javacardx.crypto, API specified by Java Card specification. Note that the PKCS#15 is purely functional and no security has been claimed.

1.4.3.9 UICC ETSI Suspension and Poll Interval Negotiation

The ETSI UICC suspension and Poll Interval Negotiation can be used by the terminal to suspend the UICC when access is not required for long periods of time, in order to reduce the overall power consumption.

This function is used to store the internal status of the UICC so that the power supply to the UICC can be switched off, and to subsequently restore the UICC status. The mechanism therefore allows restoring to a new card session certain states saved at suspension of a previous card session.

No security functionality is claimed as this is a purely functional feature.

1.4.4 Non-TOE Hardware/Software/Firmware

Here is a description of the non-TOE components and systems:

Component	Required	Description
Bytecode verifier	Mandatory	The bytecode verifier is a program that performs static checks on the bytecodes of the methods of a CAP file prior to the execution of the file on the card. Bytecode verification is a key component of security: applet isolation, for instance, depends on the file satisfying the properties a verifier checks to hold. A method of a CAP file that has been verified shall not contain, for instance, an instruction that allows forging a memory address or an instruction that makes improper use of a return address as if it were an object reference. In other words, bytecodes are verified to hold up to the intended use to which they are defined. Bytecode verification could be performed totally or partially dynamically. No standard procedure in that concern has yet been recognized. Furthermore, different approaches have been proposed for the implementation of bytecode verifiers, most notably data flow analysis, model checking and lightweight bytecode verification, this latter being an instance of what is known as proof carrying code. The actual set of checks performed by the verifier is implementation-dependent, but it is required that it should at least enforce all the "must clauses" imposed in [JCEM] on the bytecodes and the correctness of the CAP files' format.

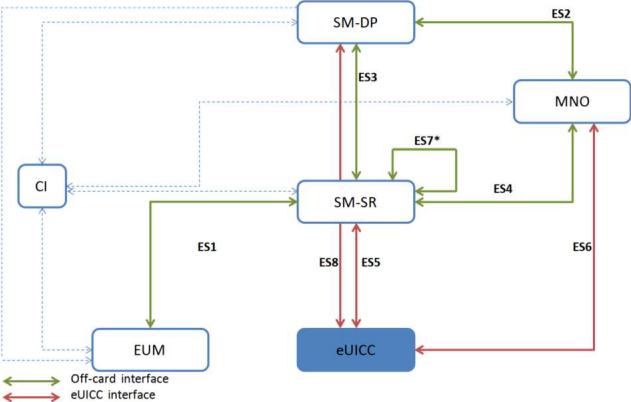
MNO-SD and applications	Mandatory	<p>The Profile controlled by each ISD-P consists in a MNO-SD security domain, which itself may manage several applications.</p> <p><i>Basic applications</i></p> <p>Basic applications stand for applications that do not require any particular security for their own.</p> <p>Basic applications must be compliant with the security rules as defined in [GP-SGBA].</p> <p><i>Secure Applications</i></p> <p>Secure applications 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.</p> <p>As such, secure applications follow a Common Criteria evaluation and certification in composition with the previously certified underlying Platform.</p>
M2M Device	Mandatory	<p>The eUICC is intended to be plugged in a M2M Device. This equipment can be a module within a car, medical equipment, camera, utility meter or any other connecting Device.</p> <p>The M2M Device may not be easily reachable, and is not expected to include a user interface, at least related to the eUICC functionality. For this reason, the eUICC does not include applications requiring user interaction such as PIN entry.</p> <p>No security certification is expected to be performed on the Device itself, and the eUICC may not rely on the Device security to protect its assets.</p>
Remote provisioning infrastructure	Mandatory	<p>The eUICC interfaces with the following remote provisioning entities, that are responsible for the management of Profiles on the eUICC.</p>  <p>The diagram illustrates the following components and their interactions:</p> <ul style="list-style-type: none"> CI (Certificate Issuer): Connected to SM-DP, SM-SR, and EUM via off-card interfaces (dashed lines). EUM (Elementary User Module): Connected to SM-SR via an off-card interface (ES1). SM-SR (Subscription Manager - Secure Routing): Connected to SM-DP (ES3), MNO (ES4), and eUICC (ES5, ES8). SM-DP (Subscription Manager - Data Protection): Connected to MNO (ES2). MNO (Mobile Network Operator): Connected to SM-DP (ES2) and SM-SR (ES4). eUICC (eUICC): Connected to SM-SR (ES5, ES8) and MNO (ES6). ES7*: An interface between two SM-SR entities for the change of SM-SR. <p>Legend: ↔ Off-card interface ↔ eUICC interface</p> <p>* Interface between two SM-SR entities for the change of SM-SR</p> <p>The TOE communicates with remote servers of</p> <ul style="list-style-type: none"> • SM-SR, which provides Platform management commands and secure routing for SMDP • SM-DP, which provides Profile management commands and Profiles • MNO OTA Platforms <p>The TOE shall require the use of secure channels for these interfaces. The keys and/or certificates required for these operations on the TOE are either provisioned onto the eUICC prior issuance, or generated post issuance, or provisioned over-the-air post issuance, depending on the interface. Identities (in terms of certificates) rely on a single root of trust called the CI (Certificate Issuer), whose public key is stored pre-issuance on the eUICC.</p> <p>The remote servers and, if any, the Devices (such a HSM) from which the keys are obtained are referred as Trusted IT products.</p>

Table 3 Components of the environment

1.4.5 TOE Life Cycle

This Security Target is conformant to [PP-eUICC]. In the following, just a summary and some useful explanations are given. For complete details on the TOE life cycle, please refer to [PP-eUICC].

The composite product life cycle is decomposed into 5 phases. Each of these phases has the very same boundaries as those defined in the claimed protection profile.

The life cycle phases are summarized in Table 4.

Phase	Name	Description
a	eUICC platform development	This phase corresponds to the first two stages of the IC development. In this phase the ST4SIM-201 OS and related applications are developed according to the Phase 1 of the ST Life cycle model as reported in Operational User Guidance.
b	eUICC platform storage, pre-persono, test Security IC manufacturing and packaging	This phase corresponds to the phases 3 and 4 of the IC development. The TOE hardware is delivered at the end of Phase 4 in packaged form. In addition, an encrypted image containing ST4SIM-201 OS and applications is delivered.
c	eUICC platform storage, pre-persono, test integration of Platform Software (JCOS, GP, policy enforcement module, telecom framework) and Applications (ECASD / ISD-R)	This phase corresponds to phase 5 of the IC development. In this phase the encrypted image is downloaded on the hardware by using the Flash Loader according to [ST-IC]. Product configuration is performed, including all the applications integration, the system applications configurations and the profile loading and configuration, according to Phase 5 of ST life cycle model reported in Operational User Guidance.
d	eUICC personalization Addition of applications (profiles / ISD-P)	This phase corresponds to phase 6 of the IC development. In this phase, the ST4SIM-201 devices are personalized with diversified credentials, according to Phase 6 of ST life cycle model reported in Operational User Guidance; this is equivalent to "Phase D" of eUICC PP TOE Delivery
e	Operational usage	This phase corresponds to phase 7 of the IC development. Such a phase represents the life cycle state of the product on the field, according to Phase 7 of ST life cycle model reported in Operational User Guidance.

Table 4 TOE life cycle phases

2 Conformance claims

2.1 CC Conformance Claims

The TOE and ST claim conformance to the CC Version 3.1 revision 5 [CC31R5P2] [CC31R5P3].
The ST claim conformance to CC Part 2 extended and CC Part 3 conformant.

2.2 Package Claims

ST claims conformance to assurance package EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

2.3 PP Claims

ST claims demonstrable conformance to:

- Embedded UICC Protection Profile v1.1 [PP-eUICC].
- Java Card Protection Profile - Open Configuration Version 3.0 [PP-JC].

2.4 Conformance Rationale

This Security Target claims demonstrable conformance to the protection profiles [PP-eUICC] and [PP-JC].

[PP-eUICC] is written to make it possible to be claimed along with [PP-JC]. The operations done for the SFRs taken from the [PP-eUICC] and [PP-JC] are clearly indicated. There are no conflicts when claiming both of them.

The Security Assurance Requirements statement for the TOE in this Security Target includes all the requirements for the TOE from the [PP-eUICC] and [PP-JC].

2.4.1 Security Problem Definition Statement

All sections of this Security Target regarding the Security Problem Definition, Security Objectives Statement and Security Requirements Statement for the TOE are taken over from the [PP-eUICC] and [PP-JC] with the exception described in the following table.

SO from [PP-JC]	Description
A.DELETION	Deletion of applets is in the scope of the evaluation. As discussed in Section 2.4.2.1, O.CARD_MANAGEMENT is now Security Objective for the TOE.

Table 5 Security Problem Definition Statement

2.4.2 Security Objectives Statement

2.4.2.1 Java Card

The Security Objectives for the TOE and its environment of the Java Card component are the same as in the Java Card PP [PP-JC]. However, the following Security Objectives for the Operational Environment have been replaced by Security Objectives for the TOE with some updates due to the fact that the Security IC is in the scope of the evaluation.

SO from [PP-JC]	Description
OE.CARD-MANAGEMENT	Request on the Security IC component. Replaced by O.CARD-MANAGEMENT.
OE.SCP.RECOVERY	Request on the Security IC component. Replaced by O.SCP.RECOVERY.
OE.SCP.SUPPORT	Request on the Security IC component. Replaced by O.SCP.SUPPORT.
OE.SCP.IC	Request on the Security IC component. Replaced by O.SCP.IC.

Table 6 Java Card security objective statement

2.4.2.2 eUICC

The Security Objectives for the TOE and its environment of the eUICC component are the same as in the eUICC PP [PP-eUICC] with some exclusions due to the overlap with the Java Card objectives defined in [PP-JC]:

SO from [PP-eUICC]	Description
OE.IC.PROOF_OF_IDENTITY	Request on the Security IC component. It is met as described in Section 1.2
OE.IC.SUPPORT	Request on the Security IC component. Covered by O.SCP.SUPPORT as discussed in Section 2.4.2.1.
OE.IC.RECOVERY	Request on the Security IC component. Covered by O.SCP.RECOVERY as discussed in Section 2.4.2.1.
OE.RE.PSF	Request on the Runtime Environment that is met by the Java Card objectives related to the threats T.DELETION and T.INSTALL defined in [PP-JC].
OE.RE.SECURE-COMM	Request on the Runtime Environment that is met by the Java Card objectives related to the following threats defined in [PP-JC]: T.CONFID-APPLI-DATA and T.INTEG-APPLI-DATA.
OE.RE.API	Request on the Runtime Environment that is met by the Java Card objectives related to the following threats defined in [PP-JC]: T.CONFID-JCS-CODE, T.INTEG-JCS-CODE, T.CONFID-JCS-DATA and T.INTEG-JCS-DATA.
OE.RE.DATA-CONFIDENTIALITY	Request on the Runtime Environment that is met by the Java Card objectives related to the following threat defined in [PP-JC]: T.CONFIDAPPLI-DATA.
OE.RE.DATA-INTEGRITY	Request on the Runtime Environment that is met by the Java Card objectives related to the following threats defined in [PP-JC]: T.INTEG-APPLI-DATA, T.INTEG-APPLIDATA.LOAD, T.INTEG-APPLI-CODE and T.INTEG-APPLI-CODE.LOAD.
OE.RE.IDENTITY	Request on the Runtime Environment that is met by the Java Card objectives related to the following threats defined in [PP-JC]: T.SID.1 and T.SID.2.
OE.RE.CODE-EXE	Request on the Runtime Environment that is met by the Java Card objectives related to the following threats defined in [PP-JC]: T.EXE-CODE.1, T.EXE-CODE.2, T.EXECODE-REMOTE and T.NATIVE.

Table 7 eUICC security objective statement

2.4.3 Security Functional Requirements Statement

2.4.3.1 Java Card

The Security Functional Requirements for the Java Card component are taken from the Java Card PP [PP-JC] without any modification. No optional features described in the Java Card PP Appendix 2 [PP-JC] are in the scope. The FCS_RNG.1 claim is combined with that of [PP-eUICC].

2.4.3.2 eUICC

The Security Functional Requirements for the eUICC component are taken from the eUICC PP [PP-eUICC] without any modification. Additionally, some SFRs have been renamed to avoid duplication with the SFRs defined in the Java Card PP [PP-JC], as shown in the following table:

SFR from [PP-eUICC]	SFR in the ST
FIA_ATD.1	FIA_ATD.1/EUICC
FIA_API.1	FIA_API.1/EUICC
FDP_SDI.1	FDP_SDI.1/EUICC
FDP_RIP.1	FDP_RIP.1/EUICC
FPT_FLS.1	FPT_FLS.1/EUICC
FMT_MSA.3	FMT_MSA.3/EUICC
FMT_SMF.1	FMT_SMF.1/EUICC
FMT_SMR.1	FMT_SMR.1/EUICC

Table 8 Renamed eUICC SFRs

3 Security Problem Definition

3.1 Java Card

The Security Problem Definition for the Java Card implementation is compliant with the Security Problem Definition described in the Java Card PP [PP-JC] with the exceptions described in Section 2.4.1.

3.2 eUICC

The Security Problem Definition for the eUICC implementation is compliant with the Security Problem Definition described in the eUICC PP [PP-eUICC].

4 Security Objectives

4.1 JavaCard

4.1.1 Security Objectives for the TOE

The Security Objectives for the TOE for the Java Card implementation are taken from the Security Objectives for the TOE described in the Java Card PP [PP-JC].

As discussed in Section 2.4.2.1, additional Security Objectives for the TOE have been added. Description is shown in the following table.

SO for the TOE	Description
O.CARD-MANAGEMENT	<p>The card manager shall control the access to card management functions such as the installation, update or deletion of applets. It shall also implement the card issuer's policy on the card.</p> <p>The card manager is an application with specific rights, which is responsible for the administration of the smart card. This component will in practice be tightly connected with the TOE, which in turn shall very likely rely on the card manager for the effective enforcing of some of its security functions. Typically the card manager shall be in charge of the life cycle of the whole card, as well as that of the installed applications (applets). The card manager should prevent that card content management (loading, installation, deletion) is carried out, for instance, at invalid states of the card or by non-authorized actors. It shall also enforce security policies established by the card issuer.</p>
O.SCP.IC	<p>The SCP shall provide all IC security features against physical attacks.</p> <p>This security objective for the environment refers to the point (7) of the security aspect #.SCP: It is required that the IC is designed in accordance with a well-defined set of policies and Standards (likely specified in another protection profile), and will be tamper resistant to actually prevent an attacker from extracting or altering security data (like cryptographic keys) by using commonly employed techniques (physical probing and sophisticated analysis of the chip). This especially matters to the management (storage and operation) of cryptographic keys.</p>
O.SCP.RECOVERY	<p>If there is a loss of power, or if the smart card is withdrawn from the CAD while an operation is in progress, the SCP must allow the TOE to eventually complete the interrupted operation successfully, or recover to a consistent and secure state.</p> <p>This security objective for the environment refers to the security aspect #.SCP(1): The smart card platform must be secure with respect to the SFRs. Then after a power loss or sudden card removal prior to completion of some communication protocol, the SCP will allow the TOE on the next power up to either complete the interrupted operation or revert to a secure state.</p>
O.SCP.SUPPORT	<p>The SCP shall support the TSFs of the TOE.</p> <p>This security objective for the environment refers to the security aspects 2, 3, 4 and 5 of #.SCP:</p> <ul style="list-style-type: none"> • (2) 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. • (3) It provides secure low-level cryptographic processing to the Java Card System. • (4) 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. <p>(5) 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).</p>

Table 9 Additional Security Objectives for the TOE

4.1.2 Security Objectives for the Operational Environment

The Security Objectives for the Operational Environment for the Java Card implementation are taken from the Security Objectives for the Operational Environment described in the Java Card PP [PP-IC] with the exceptions discussed in Section 2.4.2.1.

4.1.3 Security Objectives Rationale

The Security Objectives Rationale for the Java Card implementation are taken from the Security Objectives Rationale section described in the Java Card PP [PP-JC] with the exceptions discussed in Sections 2.4.1 and 2.4.2.1.

4.2 eUICC

4.2.1 Security Objectives for the TOE

The Security Objectives for the TOE for the eUICC implementation have been taken from the Security Objectives for the TOE described in the eUICC PP [PP-eUICC].

4.2.2 Security Objectives for the Operational Environment

The Security Objectives for the Operational Environment for the eUICC implementation have been taken from the Security Objectives for the Operational Environment described in the eUICC PP [PP-eUICC] with the exclusions discussed in 2.4.2.2.

4.2.3 Security Objectives Rationale

The Security Objectives Rationale for the eUICC implementation has been taken from the Security Objectives Rationale described in the eUICC PP [PP-eUICC] with the exceptions discussed in Sections 2.4.2.2 and 2.4.1.

5 Extended Component Definition

5.1 eUICC

Extended Component Definition has been taken with no modification from the eUICC PP [PP-eUICC].

5.2 Java Card

Extended Component Definition from the Java Card [PP-JC] overlaps with the Extended Component Definition from the eUICC PP [PP-eUICC] as it defines the FCS_RNG.1.

The ST uses the Extended Component Definition from the eUICC PP [PP-eUICC].

6 Security Functional Requirements

Reading notes:

- Selections having been made by the PP author are denoted as underlined text.
- Selections filled in by the ST author appear in square brackets with an indication that a selection is to be made [selection:] and are italicised.
- Assignments having been made by the PP author are denoted by showing as bold text.
- Assignments filled in by the ST author appear in square brackets with an indication that an assignment is to be made [assignment:] and are italicised.
- Refinements, if applicable, have been identified in bold and italicised text.
- Iteration is denoted by showing a slash “/”, and the iteration indicator after the component identifier.

6.1 Java Card

6.1.1 COREG_LC SECURITY FUNCTIONAL REQUIREMENTS

The following table shows all the SFRs from Java Card PP [PP-JC] that do not require to perform any operation and therefore are an exact copy of the PP. SFRs containing operations that have not been performed by the Java Card PP [PP-JC] are addressed in the following sections.

Section	SFR
Firewall Policy	FDP_ACC.2/FIREWALL Complete access control
	FDP_ACF.1/FIREWALL Security attribute based access control
	FDP_IFC.1/JCVM Subset information flow control
	FDP_RIP.1/OBJECTS Subset residual information protection
	FMT_MSA.1/JCRE Management of security attributes
	FMT_MSA.1/JCVM Management of security attribut
	FMT_MSA.2/FIREWALL_JCVM Secure security attributes
	FMT_MSA.3/FIREWALL Static attribute initialisation
	FMT_MSA.3/JCVM Static attribute initialisation
	FMT_SMF.1 Specification of Management Functions
	FMT_SMR.1 Security roles
Application Programming Interface	FDP_RIP.1/ABORT Subset residual information protection
	FDP_RIP.1/APDU Subset residual information protection
	FDP_RIP.1/GlobalArray Subset residual information protection
	FDP_RIP.1/bArray Subset residual information protection
	FDP_RIP.1/KEYS Subset residual information protection
	FDP_RIP.1/TRANSIENT Subset residual information protection
	FDP_ROL.1/FIREWALL Basic rollback
Card Security Management	FPT_FLS.1 Failure with preservation of secure state
AID Management	FIA_ATD.1/AID User attribute definition
	FIA_UID.2/AID User identification before any action
	FMT_MTD.1/JCRE Management of TSF data
	FMT_MTD.3/JCRE Secure TSF data

6.1.1.1 Firewall policy

6.1.1.1.1 FDP_IFF.1/JCVM Simple security attributes

FDP_IFF.1.1/JCVM The TSF shall enforce the JCVM information flow control SFP based on the following types of subject and information security attributes:

Subjects	Security attributes
S.JCVM	Currently Active Context

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

- **An operation OP.PUT(S1, S.MEMBER, I.DATA) is allowed if and only if the Currently Active Context is "Java Card RE";**
- **o other OP.PUT operations are allowed regardless of the Currently Active Context's value.**

FDP_IFF.1.3/JCVM The TSF shall enforce the [assignment: *no additional control SFP rules*].

FDP_IFF.1.4/JCVM The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *none*].

FDP_IFF.1.5/JCVM The TSF shall explicitly deny an information flow based on the following rules: [assignment: *none*].

Application Note:

The storage of temporary Java Card RE-owned objects references is runtime-enforced ([JCRE], §6.2.8.1-3).

It should be noticed that this policy essentially applies to the execution of bytecode. Native methods, the Java Card RE itself and possibly some API methods can be granted specific rights or limitations through the FDP_IFF.1.3/JCVM to FDP_IFF.1.5/JCVM elements. The way the Java Card virtual machine manages the transfer of values on the stack and local variables (returned values, uncaught exceptions) from and to internal registers is implementation-dependent. For instance, a returned reference, depending on the implementation of the stack frame, may transit through an internal register prior to being pushed on the stack of the invoker. The returned bytecode would cause more than one OP.PUT operation under this scheme.

6.1.1.2 Application Programming Interface

6.1.1.2.1 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [assignment:

see table below] and specified cryptographic key sizes [assignment: see table below] that meet the following: [assignment: see table below].

Application Note:

- The keys can be generated and diversified in accordance with [JCAPI] specification in classes KeyBuilder and KeyPair (at least Session key generation).
- This component shall be instantiated according to the version of the Java Card API applying to the security target and the implemented algorithms ([JCAPI]).

Cryptographic key generation algorithm	Cryptographic key size (in bits)	List of standards
TDES	112, 168	FIPS PUB 46-3 (ANSI X3.92), FIPS PUB 81 GlobalPlatform v2.3
ECKeyp	160 - 521	IEEE Std 1363a-2004
AES	128, 192, 256	FIPS PUB 197 [GP-B]

6.1.1.2.2 FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: see table below] that meets the following: [assignment: see table below].

Application Note:

- Command SetKEY that meets [JCAPI] specification.
- This component shall be instantiated according to the version of the Java Card API applying to the security target and the implemented algorithms ([JCAPI]).

Algorithm	Distribution Method	List of standards
AES	setKey()	Java Card API
DES/TDES	setKey()	Java Card API
ECKeyp	setS() (secret key) setA() setB() setFieldFP() setG() setK() setR() setW() (public key point)	Java Card API

6.1.1.2.3 FCS_CKM.3 Cryptographic key access

FCS_CKM.3.1 The TSF shall perform [assignment: the types of cryptographic key access described below] in accordance with a specified cryptographic key access method [assignment: cryptographic

key access method described below] that meets the following:
[assignment: *Java Card API [JCAPI]*].

- DES/AES. The following JC API key access method:
 - DES.getKey(), AES.getKey
- RSA. The following JC API key access methods:
 - RSAPrivateCRTKey.getP, RSAPrivateCRTKey.getQ, RSAPrivateCRTKey.getPQ, RSAPrivateCRTKey.getDP1, RSAPrivateCRTKey.getDQ1, RSAPrivateKey.getModulus, RSAPrivateKey.getExponent, RSAPublicKey.getModulus, RSAPublicKey.getExponent
- ECKeyP. The following JC API key access methods:
 - ECPrivateKey.getField, ECPrivateKey.getA, ECPrivateKey.getB, ECPrivateKey.getG, ECPrivateKey.getR, ECPrivateKey.getK, , ECPrivateKey.getS, ECPublicKey.setA, ECPublicKey.getField, ECPublicKey.getA, ECPublicKey.getB, ECPublicKey.getG, ECPublicKey.getR, ECPublicKey.getK, ECPublicKey.getW,

Application Note:

- The keys can be accessed as specified in [JCAPI] Key class.
- This component shall be instantiated according to the version of the Java Card API applicable to the security target and the implemented algorithms ([JCAPI], [JCAPI221], [JCAPI222] and [JCAPI3]).

6.1.1.2.4 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *overwriting the keys with zeros*] that meets the following:
[assignment: *none*].

Application Note:

- The keys are reset as specified in [JCAPI] Key class, with the method clearKey(). Any access to a cleared key for ciphering or signing shall throw an exception.
- This component shall be instantiated according to the version of the Java Card API applicable to the security target and the implemented algorithms ([JCAPI], [JCAPI221], [JCAPI222] and [JCAPI3]).

6.1.1.2.5 FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform [assignment: list of cryptographic operations in table below] in accordance with a specified cryptographic algorithm [assignment: cryptographic algorithm in table below] and cryptographic key sizes [assignment: cryptographic key sizes in table below] that meet the following:
[assignment: list of standards in table below].

Application Note:

- The TOE shall provide a subset of cryptographic operations defined in [JCAPI] (see javacardx.crypto.Cipher and javacardx.security packages).
- This component shall be instantiated according to the version of the Java Card API applicable to the security target and the implemented algorithms ([JCAPI], [JCAPI221], [JCAPI222] and [JCAPI3]).

Cryptographic operation	Cryptographic algorithm	Supported key size	Standards
Signature's verification	ECDSA	160, 192, 256, 384, 512 and 521bits	ANSI X9.62-1998
Hash functions	MD5 SHA-1 SHA-224 SHA-256 SHA-384 SHA-512 SHA-3 (KeccakP1600 used in TUAK network authentication algorithm)	NA	Secure Hash Standard, FIPS PUB 180-4 FIPS 202
Signature	HMAC	64 - 1016 bits Based on SHA-256, SHA-384 and SHA-512	FIPS 198 The Keyed-Hash Message Authentication Code (HMAC)
Signature, signature's verification, encryption and decryption	AES with Modes CBC, ECB, and CMAC	128 to 256 bits with a step of 64 bits	FIPS PUB 197 SP800-38B (CMAC)
Signature, signature's verification, encryption and decryption	DES – TDES with Modes CBC, ECB, and CMAC	56, 112 or 168 bits	FIPS PUB 46-3, ANSI X3.92, FIPS PUB 81, ISO/IEC 9797(1999), Data integrity mechanism (*)
Key agreement	ECDH	160, 192, 256, 384, 512 and 521bits	NIST 800-56A Rev.3

6.1.1.3 Card Security Management

6.1.1.3.1 FAU_ARP.1 Security alarms

FAU_ARP.1.1

The TSF shall take **one of the following actions**:

- **throw an exception,**
- **lock the card session,**
- **reinitialize the Java Card System and its data,**
- **[assignment: none]**

upon detection of a potential security violation.

Refinement:

The "potential security violation" stands for one of the following events:

- CAP file inconsistency,
- typing error in the operands of a bytecode,
- applet life cycle inconsistency,
- card tearing (unexpected removal of the Card out of the CAD) and power failure, abort of a transaction in an unexpected context, (see abortTransaction(), [JCAPI] and ([JCRE], §7.6.2)
- violation of the Firewall or JCVM SFPs,
- unavailability of resources,
- array overflow,
- [assignment: integrity error caused by a perturbation attack].

Application Note:

- The developer shall provide the exhaustive list of actual potential security violations the TOE reacts to. For instance, other runtime errors related to applet's failure like uncaught exceptions.
- The bytecode verification defines a large set of rules used to detect a "potential security violation". The actual monitoring of these "events" within the TOE only makes sense when the bytecode verification is performed on-card.
- Depending on the context of use and the required security level, there are cases where the card manager and the TOE must work in cooperation to detect and appropriately react in case of potential security violation. This behavior must be described in this component. It shall detail the nature of the feedback information provided to the card manager (like the identity of the offending application) and the conditions under which the feedback will occur (any occurrence of the java.lang.SecurityException exception).
- The "locking of the card session" may not appear in the policy of the card manager. Such measure should only be taken in case of severe violation detection; the same holds for the re-initialization of the Java Card System. Moreover, the locking should occur when "clean" re-initialization seems to be impossible.
- The locking may be implemented at the level of the Java Card System as a denial of service (through some systematic "fatal error" message or return value) that lasts up to the next "RESET" event, without affecting other components of the card (such as the card manager). Finally, because the installation of applets is a sensitive process, security alerts in this case should also be carefully considered herein

6.1.1.3.2 FDP_SDI.2 Stored data integrity monitoring and action

FDP_SDI.2.1 The TSF shall monitor user data stored in containers controlled by the TSF for [assignment: *integrity errors*] on all objects, based on the following attributes: [assignment: *integrity protected data*].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [assignment: *write a security error information persistently and mute the card*].

Application Note:

The following data elements have the user data attribute "integrity protected data":

- cryptographic keys

- PIN, PUK values
- Profile Data
- Control system variables (such as state machine information, cryptographic algorithm input data)

6.1.1.3.3 FPR_UNO.1 Unobservability

FPR_UNO.1.1 The TSF shall ensure that [assignment: *all users*] are unable to observe the operation [assignment: *all operations*] on [assignment: *D.APP_KEYS, D.PIN*] by [assignment: *all other users*]

Application Note:

Although it is not required in [JCRE] specifications, the non-observability of operations on sensitive information such as keys appears as impossible to circumvent in the smart card world. The precise list of operations and objects is left unspecified, but should at least concern secret keys and PIN codes when they exist on the card, as well as the cryptographic operations and comparisons performed on them.

6.1.1.3.4 FPT_TDC.1 Inter-TSF basic TSF data consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret **the CAP files, the bytecode and its data arguments** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use

- **the rules defined in [JCVM] specification,**
- **the API tokens defined in the export files of reference implementation,**
- [assignment: *none*]

when interpreting the TSF data from another trusted IT product.

Application Note:

Concerning the interpretation of data between the TOE and the underlying Java Card platform, it is assumed that the TOE is developed consistently with the SCP functions, including memory management, I/O functions and cryptographic functions.

6.1.1.4 AID Management

6.1.1.4.1 FIA_USB.1/AID User-subject binding

FIA_USB.1.1/AID The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **Package AID**.

FIA_USB.1.2/AID The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the

behalf of users: [assignment: *for each loaded package is associated an unique Package AID*].

FIA_USB.1.3/AID

The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: *the initially assigned Package AID is unchangeable*].

Application Note:

The user is the applet and the subject is the S.PACKAGE. The subject security attribute "Context" shall hold the user security attribute "package AID".

6.1.2 InstG Security Functional Requirements

The following table shows all the SFRs from Java Card PP [PP-JC] that do not require to perform any operation and therefore are an exact copy of the PP. SFRs containing operations that have not been performed by the Java Card PP [PP-JC] are addressed in the following sections.

Section	SFR
InstG SFRs	FDP_ITC.2/Installer Import of user data with security attributes
	FMT_SMR.1/Installer Security roles
	FPT_FLS.1/Installer Failure with preservation of secure state

6.1.2.1 FPT_RCV.3/Installer Automated recovery without undue loss

FPT_RCV.3.1/Installer	When automated recovery from [assignment: <i>none</i>] is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.
FPT_RCV.3.2/Installer	For [assignment: interrupted deletion, interrupted load or interrupted install (except if the register method has already been invoked)], the TSF shall ensure the return of the TOE to a secure state using automated procedures.
FPT_RCV.3.3/Installer	The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding [assignment: 0%] for loss of TSF data or objects under the control of the TSF.
FPT_RCV.3.4/Installer	The TSF shall provide the capability to determine the objects that were or were not capable of being recovered.

Application Note:

FPT_RCV.3.1/Installer:

- This element is not within the scope of the Java Card specification, which only mandates the behavior of the Java Card System in good working order. Further details on the "maintenance mode" shall be provided in specific implementations. The following is an excerpt from [CC2], p298: In this maintenance mode normal operation might be impossible or severely restricted, as otherwise insecure situations might occur. Typically, only authorised users should be allowed access to this mode but the real details of who can access this mode is a function of FMT: Security management. If FMT: Security management does not put any controls on who can access this mode, then it may be acceptable to allow any user to restore the system if the TOE enters such a state. However, in practice, this is probably not desirable as the user restoring the system has an opportunity to configure the TOE in such a way as to violate the SFRs.

FPT_RCV.3.2/Installer:

- Should the installer fail during loading/installation of a package/applet, it has to revert to a "consistent and secure state". The Java Card RE has some clean up duties as well; see [JCRE], §11.1.5 for possible scenarios. Precise behavior is left to

implementers. This component shall include among the listed failures the deletion of a package/applet. See ([JCRE], 11.3.4) for possible scenarios. Precise behavior is left to implementers.

- Other events such as the unexpected tearing of the card, power loss, and so on, are partially handled by the underlying hardware platform (see [PP0035]) and, from the TOE's side, by events "that clear transient objects" and transactional features. See FPT_FLS.1.1, FDP_RIP.1/TRANSIENT, FDP_RIP.1/ABORT and FDP_ROL.1/FIREWALL.

FPT_RCV.3.3/Installer:

- The quantification is implementation dependent, but some facts can be recalled here. First, the SCP ensures the atomicity of updates for fields and objects, and a power-failure during a transaction or the normal runtime does not create the loss of otherwise permanent data, in the sense that memory on a smart card is essentially persistent with this respect (EEPROM). Data stored on the RAM and subject to such failure is intended to have a limited lifetime anyway (runtime data on the stack, transient objects' contents).
According to this, the loss of data within the TSF scope should be limited to the same restrictions of the transaction mechanism.

6.1.3 ADELG Security Functional Requirements

The following table shows all the SFRs from Java Card PP [PP-JC] that do not require to perform any operation and therefore are an exact copy of the PP. SFRs containing operations that have not been performed by the Java Card PP [PP-JC] are addressed in the following sections.

Section	SFR
ADELG SFRs	FDP_ACC.2/ADEL Complete access control
	FDP_ACF.1/ADEL Security attribute based access control
	FDP_RIP.1/ADEL Subset residual information protection
	FMT_MSA.1/ADEL Management of security attributes
	FMT_MSA.3/ADEL Static attribute initialisation
	FMT_SMF.1/ADEL Specification of Management Functions
	FMT_SMR.1/ADEL Security roles
	FPT_FLS.1/ADEL Failure with preservation of secure state

6.1.4 ODELG Security Functional Requirements

The following table shows all the SFRs from Java Card PP [PP-JC] that do not require to perform any operation and therefore are an exact copy of the PP. This section does not contain any SFRs with operations still to be performed.

Section	SFR
ODELG SFRs	FDP_RIP.1/ODEL Subset residual information protection
	FPT_FLS.1/ODEL Failure with preservation of secure state

6.1.5 CarG Security Functional Requirements

The following table shows all the SFRs from Java Card PP [PP-JC] that do not require to perform any operation and therefore are an exact copy of the PP. SFRs containing operations that have not been performed by the Java Card PP [PP-JC] are addressed in the following sections.

Section	SFR
CarG SFRs	FDP_IFC.2/CM Complete information flow control
	FTP_ITC.1/CM Inter-TSF trusted channel

6.1.5.1 FCO_NRO.2/CM Enforced proof of origin

FCO_NRO.2.1/CM	The TSF shall enforce the generation of evidence of origin for transmitted application packages at all times.
FCO_NRO.2.2/CM [Editorially Refined]	The TSF shall be able to relate the identity of the originator of the information, and the application package contained in the information to which the evidence applies.
FCO_NRO.2.3/CM	The TSF shall provide a capability to verify the evidence of origin of information to recipient given [assignment: <i>at the time the Executable load files are received as no evidence is kept on the card for future verification</i>].

Application Note:

FCO_NRO.2.1/CM:

- Upon reception of a new application package for installation, the card manager shall first check that it actually comes from the verification authority. The verification authority is the entity responsible for bytecode verification.

FCO_NRO.2.3/CM:

- The exact limitations on the evidence of origin are implementation dependent. In most of the implementations, the card manager performs an immediate verification of the origin of the package using an electronic signature mechanism, and no evidence is kept on the card for future verifications.

6.1.5.2 FDP_IFF.1/CM Simple security attributes

FDP_IFF.1.1/CM	The TSF shall enforce the PACKAGE LOADING information flow control SFP based on the following types of subject and information security attributes: [assignment: <i>Load file, DAP authenticated, OTA authenticated</i>].
FDP_IFF.1.2/CM	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: <i>the rules describing the</i>

communication protocol used by the CAD and the card for transmitting a new package as detailed in [GP] Section 9.3.9).

- FDP_IFF.1.3/CM The TSF shall enforce the [assignment: *none*].
- FDP_IFF.1.4/CM The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *none*].
- FDP_IFF.1.5/CM The TSF shall explicitly deny an information flow based on the following rules:
- **The TOE fails to verify the integrity and authenticity evidences of the application package**
 - [assignment: *the rules describing the communication protocol used by the CAD and the card for transmitting a new package as detailed in [GP] Section 9.3.9).*

Application Note:

FDP_IFF.1.1/CM:

- The security attributes used to enforce the PACKAGE LOADING SFP are implementation dependent. More precisely, they depend on the communication protocol enforced between the CAD and the card. For instance, some of the attributes that can be used are: (1) the keys used by the subjects to encrypt/decrypt their messages; (2) the number of pieces the application package has been split into in order to be sent to the card; (3) the ordinal of each piece in the decomposition of the package, etc. See for example Appendix D of [GP].

FDP_IFF.1.2/CM:

- The precise set of rules to be enforced by the function is implementation dependent. The whole exchange of messages shall verify at least the following two rules: (1) the subject S.INSTALLER shall accept a message only if it comes from the subject S.CAD; (2) the subject S.INSTALLER shall accept an application package only if it has received without modification and in the right order all the APDUs sent by the subject S.CAD.

FDP_IFF.1.5/CM:

- The verification of the integrity and authenticity evidences can be performed either during loading or during the first installation of an application of the package.

6.1.5.3 FDP_UIT.1/CM Data exchange integrity

FDP_UIT.1.1/CM The TSF shall enforce the **PACKAGE LOADING information flow control SFP** to [selection: *receive*] user data in a manner protected from [selection: *modification, deletion, insertion, replay*] errors.

FDP_UIT.1.2/CM [Editorially Refined] The TSF shall be able to determine on receipt of user data, whether **modification, deletion, insertion, replay of some of the pieces of the application sent by the CAD** has occurred.

Application Note:

Modification errors should be understood as modification, substitution, unrecoverable ordering change of data and any other integrity error that may cause the application package to be installed on the card to be different from the one sent by the CAD.

6.1.5.4 FIA_UID.1/CM Timing of identification

FIA_UID.1.1/CM The TSF shall allow [assignment:

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

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

FIA_UID.1.2/CM 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 list of TSF-mediated actions is implementation-dependent, but package installation requires the user to be identified. Here by user is meant the one(s) that in the Security Target shall be associated to the role(s) defined in the component FMT_SMR.1/CM.

6.1.5.5 FMT_MSA.1/CM Management of security attributes

FMT_MSA.1.1/CM The TSF shall enforce the **PACKAGE LOADING information flow control SFP** to restrict the ability to [selection: *modify*] [assignment: *no other operations*] the security attributes [assignment: *key data, card life cycle state, secure configuration, default SELECTED configuration*] to [assignment: *card manager*].

6.1.5.6 FMT_MSA.3/CM Static attribute initialisation

FMT_MSA.3.1/CM The TSF shall enforce the **PACKAGE LOADING information flow control SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

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

6.1.5.7 FMT_SMF.1/CM Specification of Management Functions

FMT_SMF.1.1/CM The TSF shall be capable of performing the following management functions: [assignment: *key data, card life cycle state, secure configuration, default SELECTED configuration*].

6.1.5.8 FMT_SMR.1/CM Security roles

- | | |
|----------------|--|
| FMT_SMR.1.1/CM | The TSF shall maintain the roles [assignment: <i>card manager</i>]. |
| FMT_SMR.1.2/CM | The TSF shall be able to associate users with roles. |

6.2 eUICC

The following table shows all the SFRs from eUICC PP [PP-eUICC] that do not require to perform any operation and therefore are an exact copy of the PP. SFRs containing operations that have not been performed by the eUICC PP [PP-eUICC] are addressed in the following sections.

Section	SFR
Identification and authentication	FIA_USB.1/EXT User-subject binding
	FIA_UAU.4/EXT Single-use authentication mechanisms
	FIA_UID.1/MNO-SD Timing of identification
	FIA_USB.1/MNO-SD User-subject binding
	FIA_ATD.1/EUICC User attribute definition
	FIA_API.1/EUICC Authentication Proof of Identity
Communication	FDP_IFC.1/SCP Subset information flow control
	FDP_UCT.1/SCP Basic data exchange confidentiality
	FDP_UIT.1/SCP Data exchange integrity
	FCS_CKM.1/SCP-SM Cryptographic key generation
Security Domain	FDP_ACC.1/ISDR Subset access control
	FDP_ACC.1/ISDP Subset access control
	FDP_ACC.1/ECASD Subset access control
	FDP_ACF.1/ECASD Security attribute based access control
Platform Services	FDP_IFC.1/Platform_services Subset information flow control
Security Management	FDP_SDI.1/EUICC Stored data integrity monitoring
	FDP_RIP.1/EUICC
	FPT_FLS.1/EUICC Failure with preservation of secure state
	FMT_MSA.1/PSF_DATA Management of security attributes
	FMT_MSA.1/POL1 Management of security attributes
	FMT_MSA.1/CERT_KEYS Management of security attributes
	FMT_MSA.3/EUICC Static attribute initialisation
	FMT_SMR.1/EUICC Security roles

6.2.1 Identification and authentication

6.2.1.1 FIA_UID.1/EXT Timing of identification

- FIA_UID.1.1/EXT The TSF shall allow
- **application selection**
 - **requesting data that identifies the eUICC**
 - [assignment: *no additional TSF mediated actions*].
- on behalf of the user to be performed before the user is identified.
- FIA_UID.1.2/EXT The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note 28:

This SFR is related to the identification of the following external (remote) users of the TOE:

- U.SM-SR
- U.SM-DP
- U.MNO-OTA The identification of the only local user (U.MNO-SD) is addressed by the FIA_UID.1/MNO-SD SFR.

Application selection is authorized before identification since it may be required to provide the identification of the eUICC to the remote user.

6.2.1.2 FIA_UAU.1/EXT Timing of authentication

- FIA_UAU.1.1/EXT The TSF shall allow
- **application selection**
 - **requesting data that identifies the eUICC**
 - **user identification**
 - [assignment: *no additional TSF mediated actions*].
- on behalf of the user to be performed before the user is authenticated.
- FIA_UAU.1.2/EXT The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application Note 29:

This SFR is related to the authentication of external (remote) users of the TOE:

- U.SM-SR
- U.SM-DP
- U.MNO-OTA

Regarding the use of ECDSA signature verification, the underlying elliptic curve cryptography must be compliant with one of the following:

- NIST P-256 (FIPS PUB 186-3 Digital Signature Standard)
- brainpoolP256r1 (BSI TR-03111, Version 1.11, RFC 5639)
- FRP256V1 (ANSSI ECC FRP256V1).

6.2.2 Communication

6.2.2.1 FDP_IFF.1/SCP Simple security attributes

- FDP_IFF.1.1/SCP The TSF shall enforce the Secure Channel Protocol Information flow control SFP based on the following types of subject and information security attributes:
- **o users/subjects:**
 - **U.SM-SR and S.ISD-R, with security attribute D.ISDR_KEYS**
 - **U.SM-DP and S.ISD-P, with security attribute D.ISDP_KEYS**
 - **U.MNO_OTA and U.MNO-SD, with security attribute D.MNO_KEYS**
 - **information: transmission of commands.**
- FDP_IFF.1.2/SCP The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:
- **The TOE shall permit communication between U.MNO_OTA and U.MNOSD in a SCP80 or SCP81 secure channel.**
- FDP_IFF.1.3/SCP The TSF shall enforce the [assignment: *no additional information flow control SFP rules*].
- FDP_IFF.1.4/SCP The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *none*].
- FDP_IFF.1.5/SCP The TSF shall explicitly deny an information flow based on the following rules:
- **The TOE shall reject communication between U.SM-SR and S.ISD-R if it is not performed in a SCP80 or SCP81 secure channel through SMS, CAT_TP or HTTPS**
 - **o The TOE shall reject communication between U.SM-DP and S.ISD-P if it is not performed in a SCP03(t) secure channel, through the tunnel previously created between U.SM-SR and S.ISD-R.**

Application Note 35:

More details on the secure channels can be found in [SGP.02]

- For SM-SR: section 2.2.5.1 and section 2.4
- For SM-DP: section 2.2.5.2 and section 2.5
- For MNO-SD: section 2.2.5.3 and section 2.7

6.2.2.2 FTP_ITC.1/SCP Inter-TSF trusted channel

FTP_ITC.1.1/SCP	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/SCP	The TSF shall permit <u>another trusted IT</u> product to initiate communication via the trusted channel.
FTP_ITC.1.3/SCP	<p>The TSF shall initiate communication via the trusted channel for [assignment:</p> <ul style="list-style-type: none"> • <i>ES5.CreateISDP</i> • <i>ES8.EstablishISDPKeySet</i> command, followed by <i>ES8.DownloadAndInstallation</i> command • <i>ES5.EnableProfile</i> • <i>ES5.DisableProfile</i> • <i>ES5.DeleteProfile</i> • <i>ES5.eUICCCapabilityAudit</i> • <i>ES5.MasterDelete</i> • <i>ES5.SetFallbackAttribute</i> • <i>ES5.HandleNotificationConfirmation</i> • <i>ES5.EstablishISDRKeySet</i> • <i>ES5.FinaliseISDRhandover</i> • <i>ES5.UpdateSMSRAddressingParameters</i> • <i>ES8.UpdateConnectivityParameters</i> • <i>ES6.UpdatePOL1byMNO</i> • <i>ES6.UpdateConnectivityParametersByMNO</i> • <i>ES5.HandleDefaultNotification</i> <p>].</p>

Application Note 36:

Related keys are:

- either generated on-card during Profile download or SM-SR handover (D.ISDP_KEYS, D.ISDR_KEYS); see FCS_CKM.1/SCP-SM for further details
- or distributed along with the profile (D.MNO_KEYS); see FCS_CKM.2/SCP-MNO for further details

In terms of commands, the TSF shall permit remote actors to initiate communication via a trusted channel in the following cases:

The TSF shall permit the SM-SR to open a SCP80 secure channel to perform Profile Download and Installation, divided in the following steps:

- The TSF shall permit the SM-SR to transmit a *ES5.CreateISDP* command;
- The TSF shall then permit the SM-DP to open a SCP03(t) secure channel to transmit
 - a *ES8.EstablishISDPKeySet* command, followed by
 - a *ES8.DownloadAndInstallation* command;
- The TSF shall permit the SM-SR to transmit a *ES5.EnableProfile* command (optional)

The TSF shall permit the SM-SR to open a SCP80 secure channel to transmit the following Platform Management commands:

- ES5.EnableProfile
- ES5.DisableProfile
- ES5.DeleteProfile
- ES5.eUICCCapabilityAudit
- ES5.MasterDelete
- ES5.SetFallbackAttribute
- ES5.HandleNotificationConfirmation

The TSF shall permit the SM-SR to open a SCP80 secure channel to transmit the following eUICC management commands:

- ES5.EstablishISDRKeySet
- ES5.FinaliseISDRhandover
- ES5.UpdateSMSRAddressingParameters

The TSF shall permit the SM-SR to open a SCP80 secure channel to modify the connectivity parameters of the SM-DP:

- The TSF shall then permit the SM-DP to open a SCP03(t) secure channel to transmit a ES8.UpdateConnectivityParameters SCP03 command

The TSF shall permit the remote OTA Platform to open a SCP80 secure channel to transmit the following Profile management operations:

- ES6.UpdatePOL1byMNO
- ES6.UpdateConnectivityParametersByMNO

In terms of commands, the TSF shall initiate communication via the trusted channel for:

- ES5.HandleDefaultNotification

6.2.2.3 FDP_ITC.2/SCP Import of user data with security attributes

FDP_ITC.2.1/SCP	The TSF shall enforce the Secure Channel Protocol information flow control SFP when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2/SCP	The TSF shall use the security attributes associated with the imported user data.
FDP_ITC.2.3/SCP	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/SCP	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/SCP	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [assignment: <i>none</i>].

6.2.2.4 FPT_TDC.1/SCP Inter-TSF basic TSF data consistency

- FPT_TDC.1.1/SCP The TSF shall provide the capability to consistently interpret
- **Commands from U.SM-SR, U.SM-DP and U.MNO-OTA**
 - **Downloaded objects from U.SM-SR, U.SM-DP and U.MNO-OTA**
- when shared between the TSF and another trusted IT product.
- FPT_TDC.1.2/SCP The TSF shall use *[assignment: rules defined in [SGP.02]]* when interpreting the TSF data from another trusted IT product.

Application Note 37:

The commands related to the SFRs FPT_TDC.1/SCP, FDP_IFC.1/SCP, FDP_IFC.1/SCP and the Downloaded objects related to this SFR FPT_TDC.1/SCP are listed below:

- SM-SR commands
 - ES5.CreateISDP
 - ES5.EnableProfile
 - ES5.DisableProfile
 - ES5.DeleteProfile
 - ES5.eUICCCapabilityAudit
 - ES5.MasterDelete
 - ES5.SetFallbackAttribute
 - ES5.EstablishISDRKeySet
 - ES5.FinaliseISDRhandover
 - ES5.UpdateSMSRAddressingParameters
- Downloaded objects from SM-SR
 - Platform management keysets
- SM-DP commands
 - ES8.EstablishISDPKeySet
 - ES8.DownloadAndInstallation
 - ES8.UpdateConnectivityParameters SCP03
- Downloaded objects from SM-DP
 - Profile management keysets
 - MNO profiles
- MNO commands
 - ES6.UpdatePOL1byMNO
 - ES6.UpdateConnectivityParametersByMNO
- Downloaded objects from MNO OTA Platform
 - POL1 data
 - Connectivity parameters

6.2.2.5 *FCS_CKM.2/SCP-MNO Cryptographic key distribution*

- FCS_CKM.2.1/SCP-MNO The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *[assignment: cryptographic key distribution method in table*

below] that meets the following: [assignment: list of standards in table below].

Application Note 41:

This SFR is related to the distribution of

- D.MNO_KEYS during profile download
- Public keys distributed in the user certificates (CERT.SR.ECDSA and CERT.DP.ECDSA) or loaded pre-issuance of the TOE (D.eUICC_CERT, D.CI_ROOT_PUBKEY)

Application Note 42:

This SFR does not apply to the private keys loaded pre-issuance of the TOE (D.eUICC_PRIVKEY).

Algorithm	Distribution Method	List of standards
AES	SCP80 SCP81 STORE DATA functionality of security domain	[TS 102 225] [TS 102 226] [GP-B] [SGP.02] [GP]
ECDH/ECDSA	ES5.EstablishISDRKeySet ES8.EstablishISDPKeySet	[SGP.02]
TDES	STORE DATA functionality of security domain	[GP]
TUAK	[SGP.02]	[SGP.02] [TUAK]
MILENAGE	GSMA, SGP.02	[SGP.02] [MILENAGE]

6.2.2.6 FCS_CKM.4/SCP-SM Cryptographic key destruction

FCS_CKM.4.1/SCP-SM The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *overwriting the keys with zeros*] that meets the following: [assignment: *none*].

Application Note 43:

This SFR is related to the destruction of the following keys:

- D.ISDP_KEYS
- D.ISDR_KEYS
- CERT.SR.ECDSA
- CERT.DP.ECDSA
- D.eUICC_CERT,
- D.eUICC_PRIVKEY,
- D.CI_ROOT_PUBKEY,.

6.2.2.7 FCS_CKM.4/SCP-MNO Cryptographic key destruction

FCS_CKM.4.1/SCP-MNO The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *overwriting the keys with zeros*] that meets the following: [assignment: *none*].

Application Note 44:

This SFR is related to the destruction of the following keys:

- D.MNO_KEYS.

6.2.3 Security Domains

6.2.3.1 FDP_ACF.1/ISDR Security attribute based access control

FDP_ACF.1.1/ISDR The TSF shall enforce the **ISD-R access control SFP** to objects based on the following:

- **subjects: S.ISD-R**
- **objects:**
 - **S.ISD-R with security attribute "state"**
 - **S.ISD-P with security attributes "state", "fallback" and "POL1"**
- **operations:**
 - **Create (S.ISD-P)**
 - **Enable (S.ISD-P)**
 - **Disable (S.ISD-P)**
 - **Delete (S.ISD-P)**
 - **Set the fallback attribute (S.ISD-P)**
 - **Perform a capability audit (S.ISD-P)**
 - **Perform a Master Delete (S.ISD-P)**
 - **Updating the SM-SR addressing parameters (S.ISD-R)**
 - **Finalizing the SM-SR handover (S.ISD-R).**

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

- **Enabling a S.ISD-P is authorized only if**
 - **the corresponding S.ISD-P is in the state "DISABLED" and**
 - **the previously enabled S.ISD-P is in the state "DISABLED"**
- **Disabling a S.ISD-P is authorized only if**
 - **the corresponding S.ISD-P is in the state "ENABLED" or "PERSONALIZED" and**
 - **the corresponding S.ISD-P's POL1 data allows its disabling and**
 - **the corresponding S.ISD-P's fallback attribute is not set.**

- **Deleting a S.ISD-P is authorized only if**
 - the corresponding S.ISD-P is not in the state "ENABLED" and
 - the corresponding S.ISD-P's POL1 data allows its deletion and
 - the corresponding S.ISD-P's fallback attribute is not set.
- **Performing a S.ISD-P Master Delete is authorized only if**
 - the corresponding S.ISD-P is in the state "DISABLED" and
 - the corresponding S.ISD-P's fallback attribute is not set and
 - the corresponding S.ISD-P has successfully verified the U.SM-DP token transmitted with the command;.

FDP_ACF.1.3/ISDR

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *[assignment:*

- *CreateISDP (Creating an ISD-P)*
- *EnableProfile (Enabling a profile)*
- *DisableProfile (Disabling a profile)*
- *DeleteProfile (Deleting a profile)*
- *eUICCCapabilityAudit (Performing a capability audit)*
- *MasterDelete (Performing a Master Delete)*
- *SetFallbackAttribute (Setting the fallback attribute)*
- *UpdateSMSRAAddressingParameters (Updating the SM-SR addressing parameters)*
- *FinaliseISDRhandover (Finalizing the SM-SR handover)*

].

FDP_ACF.1.4/ISDR

The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- **Any of the following operations is rejected if S.ISD-R is not in the state "PERSONALIZED":**
 - **Creating an ISD-P**
 - **Performing a capability audit on a S.ISD-P**
 - **Setting the fallback attribute of a S.ISD-P**
 - **Updating the SM-SR addressing parameters on the S.ISD-R**
 - **Finalizing the SM-SR handover on the S.ISD-R**
- **Any operation on S.ISD-R is forbidden to other subjects than S.ISD-R.**

Application Note 46:

This policy describes the rules to be applied to access Platform Management or eUICC Management operations. It covers the access to all operations by ISD-R required by sections 3.x of [SGP.02], that is:

- CreateISDP (Creating an ISD-P)
- EnableProfile (Enabling a profile)
- DisableProfile (Disabling a profile)
- DeleteProfile (Deleting a profile)
- eUICCCapabilityAudit (Performing a capability audit)
- MasterDelete (Performing a Master Delete)
- SetFallbackAttribute (Setting the fallback attribute)
- UpdateSMSRAddressingParameters (Updating the SM-SR addressing parameters)
- FinaliseISDRhandover (Finalizing the SM-SR handover)

Identification and authentication SFRs (FIA_*/EXT) require that these operations are only available for the legitimate user U.SM-SR after being authenticated.

6.2.3.2 FDP_ACF.1/ISDP Security attribute based access control

FDP_ACF.1.1/ISDP The TSF shall enforce the ISD-P access control SFP to objects based on the following:

subjects:

- S.ISD-P

objects:

- Profile data (received from U.SM-DP)
- S.ISD-P with security attribute "state"

operations:

- Download and install (Profile data)
- Establish keyset (S.ISD-P)
- Update the POL1 data (S.ISD-P)
- Update the ISD-P connectivity parameters using SCP03(t) (S.ISD-P)
 - Update the ISD-P connectivity parameters by MNO (S.ISD-P).

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

- Downloading and installing profile data is authorized only if S.ISD-P's attribute "state" is "PERSONALIZED"
- Establishing a D.ISDP_KEYS keyset is authorized if S.ISD-P's attribute "state" is at least "SELECTABLE"
- Updating POL1 is authorized only if S.ISD-P's attribute "state" is "ENABLED"

- **Updating the ISD-P connectivity parameters by SCP03(t) is authorized only if S.ISD-P's attribute "state" is "ENABLED"**
- **o Updating the ISD-P connectivity parameters by MNO is authorized only if S.ISD-P's attribute "state" is "PERSONALIZED".**

FDP_ACF.1.3/ISDP The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment:

- *DownloadAndInstallation (Downloading and installing a profile)*
- *EstablishISDPKeySet (Establishing a D.ISDP_KEYS keyset)*
- *UpdateConnectivityParameters SCP03 (Updating the ISD-P connectivity parameters using SCP03(t))*
- *POL1 update (updating the POL1 data)*
- *UpdateConnectivityParametersByMNO (Connectivity Parameters Update by MNO)*

].

FDP_ACF.1.4/ISDP The TSF shall explicitly deny access of subjects to objects based on the following additional rules:

- **Any operation on Profile data or S.ISD-P is forbidden to other subjects than S.ISD-P.**

Application Note 48:

This policy describes the rules to be applied during profile management operations. It covers SM-DP operations described in [SGP.02]:

- DownloadAndInstallation (Downloading and installing a profile)
- EstablishISDPKeySet (Establishing a D.ISDP_KEYS keyset)
- UpdateConnectivityParameters SCP03 (Updating the ISD-P connectivity parameters using SCP03(t))

Identification and authentication SFRs (FIA_*/EXT) require that these operations are only available for the legitimate user U.SM-DP after being authenticated.

It also covers the MNO operations described in [SGP.02]:

- POL1 update (updating the POL1 data)
- UpdateConnectivityParametersByMNO (Connectivity Parameters Update by MNO)

Identification and authentication SFRs (FIA_*/EXT and FIA_*/MNO-SD) require that these operations are only available for the legitimate user U.MNO-OTA, via the local user U.MNOSD, after being authenticated.

6.2.4.1 FDP_IFF.1/Platform_services Simple security attributes

FDP_IFF.1.1/Platform_services	<p>The TSF shall enforce the Platform services information flow control SFP based on the following types of subject and information security attributes:</p> <p>users/subjects:</p> <ul style="list-style-type: none">• S.ISD-R, S.ISD-P, U.MNO-SD, with security attribute "application identifier (AID)" <p>information:</p> <ul style="list-style-type: none">• D.PROFILE-NAA-PARAMS• D.PROFILE-POL1 <p>operations:</p> <ul style="list-style-type: none">• installation of a profile• POL1 enforcement• o network authentication.
FDP_IFF.1.2/Platform_services	<p>The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:</p> <ul style="list-style-type: none">• D.PROFILE-NAA-PARAMS shall be transmitted only:<ul style="list-style-type: none">○ by U.MNO-SD to S.TELECOM in order to execute the "Network authentication" API function○ by S.ISD-P to S.PSF using the "Installation" API function• D.PROFILE-POL1 shall be transmitted only<ul style="list-style-type: none">○ by S.ISD-P to S.PSF in order to execute the "POL1 enforcement" function.
FDP_IFF.1.3/Platform_services	<p>The TSF shall enforce the [assignment: <i>no additional information flow control SFP rules</i>].</p>
FDP_IFF.1.4/Platform_services	<p>The TSF shall explicitly authorise an information flow based on the following rules: [assignment: <i>none</i>].</p>
FDP_IFF.1.5/Platform_services	<p>The TSF shall explicitly deny an information flow based on the following rules: [assignment: <i>none</i>].</p>

Application Note 49:

This SFR aims to control which subject is able to transmit POL1 or network authentication keys to the PSF and Telecom Framework.

6.2.4.2 FPT_FLS.1/Platform_Services Failure with preservation of secure state

FPT_FLS.1.1/Platform_Services	<p>The TSF shall preserve a secure state when the following types of failures occur:</p> <ul style="list-style-type: none">• failure that lead to a potential security violation during the processing of a S.PSF or S.TELECOM API specific functions:
-------------------------------	---

- **Installation of a profile**
- **POL1 enforcement**
- **Network authentication**
- [assignment: *none*].

6.2.5 Security management

6.2.5.1 FCS_RNG.1 Random number generation

- FCS_RNG.1.1 The TSF shall provide a [selection: *physical*] random number generator [selection: *PTG.2*] that implements: [assignment:
- (PTG.2.1) A total failure test detects a total failure of entropy source immediately when the RNG has started. When a total failure is detected, no random numbers will be output.
 - (PTG.2.2) If a total failure of the entropy source occurs while the RNG is being operated, the RNG prevents the output of any internal random number that depends on some raw random numbers that have been generated after the total failure of the entropy source.
 - (PTG.2.3) The online test shall detect non-tolerable statistical defects of the raw random number sequence (i) immediately when the RNG has started, and (ii) while the RNG is being operated. The TSF must not output any random numbers before the power-up online test has finished successfully or when a defect has been detected.
 - (PTG.2.4) The online test procedure shall be effective to detect non-tolerable weaknesses of the random numbers soon.
 - (PTG.2.5) The online test procedure checks the quality of the raw random number sequence. It is triggered externally. The online test is suitable for detecting non-tolerable statistical defects of the statistical properties of the raw random numbers within an acceptable period of time.
-].
- FCS_RNG.1.2 The TSF shall provide **octets of bits** that meet [assignment:
- (PTG.2.6) Test procedure A does not distinguish the internal random numbers from output sequences of an ideal RNG.
 - (PTG.2.7) The average Shannon entropy per internal random bit exceeds 0.997.
-].

Application Note 51:

If the ST writer selects a RNG class requiring self-test, a dedicated FPT_TST.1 SFR must also be included to describe this self-test.

6.2.5.2 FCS_COP.1/DRBG Cryptographic Operation

FCS_COP.1/DRBG The TSF shall perform the [assignment: *DRBG SHA-256*] in accordance with a specified cryptographic algorithm [assignment: *Hash-DRBG*] and cryptographic key sizes [assignment: *none*] that meet the following: [assignment: *[NISTSP800-90] and [FIPS 180-2]*].

6.2.5.3 FPT_EMS.1 TOE Emanation

FPT_EMS.1.1 The TOE shall not emit [assignment: *information about chip power consumption, electromagnetic emanation or command execution time*] in excess of [assignment: *useless information*] enabling access to

- **D.SECRETS;**
- **D.eUICC_PRIVKEY**

and **the secret keys which are part of the following keysets:**

- **D.MNO_KEYS,**
- **D.ISDR_KEYS,**
- **D.ISDP_KEYS,**
- **D.PROFILE_NAA_PARAMS.**

FPT_EMS.1.2 The TSF shall ensure [assignment: *unauthorized users*] are unable to use the following interface [assignment: *VCC, GND, I/O pads and RF field*] to gain access to

- **D.SECRETS;**
- **D.eUICC_PRIVKEY**

and **the secret keys which are part of the following keysets:**

- **D.MNO_KEYS,**
- **D.ISDR_KEYS,**
- **D.ISDP_KEYS,**
- **D.PROFILE_NAA_PARAMS.**

Application Note 52:

The TOE shall prevent attacks against the secret data of the TOE where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may originate from internal operation of the TOE or may originate from an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE.

Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission. Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to, evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, and so on.

6.2.5.4 FMT_SMF.1/EUICC Specification of Management Functions

FMT_SMF.1.1/EUICC The TSF shall be capable of performing the following management functions: [assignment: *profile management functions described in [SGP.02]*].

6.2.6 Mobile Network authentication

6.2.6.1 FCS_COP.1/Mobile_network Cryptographic operation

FCS_COP.1.1/Mobile_network The TSF shall perform **Network authentication** in accordance with a specified cryptographic algorithm **MILENAGE**, [selection: Tuak, *no other algorithm*] and cryptographic key sizes **according to the corresponding standard** that meet the following:

- **MILENAGE according to standard [MILENAGE] with the following restrictions:**
 - **Only use 128-bit AES as the kernel function – do not support other choices**
 - **Allow any value for the constant OP**
 - **Allow any value for the constants C1-C5 and R1-R5, subject to the rules and recommendations in section 5.3 of the standard [MILENAGE]**
- **Tuak according to [TUAK] with the following restrictions:**
 - **Allow any value of TOP**
 - **Allow multiple iterations of Keccak**
 - **Support 256-bit K as well as 128-bit**
 - **To restrict supported sizes for RES, MAC, CK and IK to those currently supported in 3GPP standards.**

Application Note 56:

The ST writer must list the complete list of algorithms supported by the telecom framework of the TOE (for example Milenage, and so on)

The keys used by these algorithms are distributed within the profiles during provisioning (FDP_ITC.1/SCP) and must be securely deleted (FCS_CKM.4/Mobile_network)

6.2.6.2 FCS_CKM.2/Mobile_network Cryptographic key distribution

FCS_CKM.2.1/Mobile_network The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [assignment: *cryptographic key distribution method in table below*] that meets the following: [assignment: *list of standards in table below*].

Application Note 57:

The keys in this SFR are the Mobile Network authentication keys included in the asset D.PROFILE_NAA_PARAMS. These keys are distributed as a part of the MNO profile during profile download

Algorithm	Distribution Method	List of standards
AES	SCP80 SCP81 STORE DATA functionality of security domain	[TS 102 225] [TS 102 226] [GP-B] [SGP.02] [GP]
ECDH/ECDSA	ES5.EstablishISDRKeySet ES8.EstablishISDPKeySet	[SGP.02]
TDES	STORE DATA functionality of security domain	[GP]
TUAK	[SGP.02]	[SGP.02] [TUAK]
MILENAGE	GSMA, SGP.02	[SGP.02] [MILENAGE]

6.2.6.3 FCS_CKM.4/Mobile_network Cryptographic key destruction

FCS_CKM.4.1/Mobile_network The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment: *overwriting the keys with zeros*] that meets the following: [assignment: *none*].

7 Security Assurance Requirements

This Security Target claims conformance to EAL4 augmented with AVA_VAN.5 and ALC_DVS.2. ADV_ARC is refined.

The requirements are summarised in the following table:

Assurance Class	Component	Component Title
ADV Development	ADV_ARC.1	Security architecture <i>NOTE:</i> This component has been refined as follows: <i>ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.</i> <i>Refinement:</i> <i>In particular, the TOE shall maintain the applet isolation without requiring more rules on applet verification than the [GP-SGBA].</i>
	ADV_FSP.4	Complete functional specification
	ADV_IMP.1	Implementation representation of the TSF
	ADV_TDS.3	Basic modular design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC_ Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.2	Sufficiency of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_TSS.1	TOE summary specification
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional tests
	ATE_IND.2	Independent testing
AVA: Vulnerability assessment	AVA_VAN.5	Advanced methodical vulnerability analysis

Table 10 EAL4 requirements description extended with augmented with AVA_VAN.5 and ALC_DVS.2

8 TOE Summary Specification

8.1 Security Functionality

8.1.1 Java Card

<p>SF.FIREWALL</p>	<p>The TOE implements an applet firewall according to [JCRE]. Each applet on the TOE must have been passed the Bytecode Verifier in order to ensure correct applet isolation. As an additional defensive security feature also a type check for API array parameters is performed.</p> <p>This TSF enforces the following SFRs:</p> <ul style="list-style-type: none"> • FDP_ACC.2/FIREWALL Complete access control • FDP_ACF.1/FIREWALL Security attribute based access control • FDP_IFC.1/JCVM Subset information flow control • FDP_IFF.1/JCVM Simple security attributes • FMT_MSA.1/JCRE Management of security attributes • FMT_MSA.2/FIREWALL_JCVM Secure security attributes • FMT_MSA.3/FIREWALL Static attribute initialisation • FMT_MSA.3/JCVM Static attribute initialization • FMT_SMR.1 Security roles • FDP_ROL.1/FIREWALL Basic rollback • FMT_MSA.1/JCVM Management of security attributes • FMT_MTD.1/JCRE Management of TSF data • FMT_MTD.3/JCRE Secure TSF data • FMT_SMF.1 Specification of Management Functions
<p>SF.RIP</p>	<p>This TSF ensures that sensitive information is made unavailable after deletion. This will be done by overwriting keys, APDU buffer and transient objects with zeros or random values. Applications and persistent objects will be marked as deleted. If the deleted resource is reused by a new object creation, the previous content will be set to a random value.</p> <p>This TSF enforces the following SFRs:</p> <ul style="list-style-type: none"> • FDP_RIP.1/bArray Subset residual information protection • FDP_RIP.1/APDU Subset residual information protection • FDP_RIP.1/KEYS Subset residual information protection • FDP_RIP.1/TRANSIENT Subset residual information protection • FDP_RIP.1/ADEL Subset residual information protection • FDP_RIP.1/ODEL Subset residual information protection • FDP_RIP.1/ABORT Subset residual information protection • FDP_RIP.1/OBJECTS Subset residual information protection • FDP_RIP.1/GlobalArray Subset residual information protection
<p>SF.Rollback</p>	<p>The TOE implements atomicity and rollback mechanism for Java Card runtime environment [JCRE] and GlobalPlatform management functions (see [GP]).</p> <p>The TOE also ensures that objects created during an aborted transaction are made unavailable.</p> <p>This TSF enforces the following SFRs:</p> <ul style="list-style-type: none"> • FPT_RCV.3/Installer Automated recovery without undue loss • FDP_ROL.1/FIREWALL Basic rollback • FDP_RIP.1/ABORT Subset residual information protection
<p>SF.SCP</p>	<p>The TOE implements secure channel protocols according to [GP v23], chapter 10. The following protocols are supported:</p> <ul style="list-style-type: none"> • SCP02 according to [GP-E]. • SCP03 according to [GP-D]. • SCP03t according to [GP-D] and [SGP.02]. • SCP80 according to [TS 102 225] and [TS 102 226] and supporting secure messaging over SMS and CAT_TP. • SCP81 according to [GP-B]. <p>The SCP uses as the basic cryptographic primitives the security hardened symmetric cryptographic library which is CC certified together with the underlying platform.</p> <p>This TSF enforces the following SFRs:</p>

	<ul style="list-style-type: none"> • FDP_UIT.1/CM Data exchange integrity • FTP_ITC.1/CM Inter-TSF trusted channel • FCO_NRO.2/CM Enforced proof of origin • FDP_IFC.2/CM Complete information flow control • FDP_IFF.1/CM Simple security attributes • FMT_MSA.1/CM Management of security attributes • FMT_MSA.3/CM Static attribute initialisation • FMT_SMF.1/CM Specification of Management Functions • FIA_UID.1/CM Timing of identification • FMT_SMR.1/CM Security roles • FCS_COP.1 Cryptographic operation
SF.CM	<p>The TOE implements an access control policy for GlobalPlatform card management functions according to [GP] and GlobalPlatform Amendments A [GP-A], B [GP-B], C [GP-C], D [GP-D] and E [GP-E].</p> <p>In addition to the GP specification, the Java Card Runtime Environment specification [JCRE] is followed to support for application loading, installation, and deletion.</p> <p>AID management is provided by SF.CM according to the GlobalPlatform Specification [GP], the Java Card Runtime Environment Specification [JCRE], and the Java Card API Specification [JCAPI].</p> <p>This TSF enforces the following SFRs:</p> <ul style="list-style-type: none"> • FMT_MSA.1/CM Management of security attributes • FMT_MSA.3/CM Static attribute initialisation • FMT_SMF.1/CM Specification of Management Functions • FMT_SMR.1/CM Security roles • FPT_TDC.1 Inter-TSF basic TSF data consistency • FIA_ATD.1/AID User attribute definition • FIA_UID.2/AID User identification before any action • FIA_USB.1/AID User-subject binding • FDP_ITC.2/Installer Import of user data with security attributes • FMT_SMR.1/Installer Security roles • FPT_RCV.3/Installer Automated recovery without undue loss • FPT_FLS.1/Installer Failure with preservation of secure state • FDP_ACC.2/ADEL Complete access control • FDP_ACF.1/ADEL Security attribute based access control • FDP_RIP.1/ADEL Subset residual information protection • FMT_MSA.1/ADEL Management of security attributes • FMT_MSA.3/ADEL Static attribute initialisation • FMT_SMR.1/ADEL Security roles • FPT_FLS.1/ADEL Failure with preservation of secure state • FMT_SMF.1/ADEL Specification of Management Functions • FPT_FLS.1/ADEL Failure with preservation of secure state
SF.Physical	<p>The TOE provides means to protect SFRs against physical tampering and leakage. The TOE uses mainly the physical security measures of the underlying hardware platform.</p> <p>Security mechanisms involved in this protection are:</p> <ul style="list-style-type: none"> • Memories scrambling and encryption • Protection of NVM sectors • Memory Protection Unit (MPU) • Library Protection Unit (LPU) <p>This TSF enforces the following SFRs:</p> <ul style="list-style-type: none"> • FAU_ARP.1 Security alarms • FDP_SDI.2 Stored data integrity monitoring and action • FPT_TST.1 TSF testing • FPT_FLS.1 Failure with preservation of secure state
SF.CRYPTO	<p>The TOE provides key creation, key management, key deletion and cryptographic functionality. It provides the API in accordance to the Java Card API Specification [JCAPI].</p> <p>The cryptographic API uses as the basic cryptographic implementation the security hardened cryptographic library which is CC certified together with the underlying platform.</p>

	<p>The integrity of the cryptographic assets is monitored. In addition, key destructions and residual information purging is implemented.</p> <p>SF.CRYPTO provides secure random number generation and makes this functionality available through an API according to the Java Card API Specification [JCAPI].</p> <p>This TSF enforces the following SFRs:</p> <ul style="list-style-type: none"> • FCS_CKM.1 Cryptographic key generation • FCS_CKM.2 Cryptographic key distribution • FCS_CKM.3 Cryptographic key access • FCS_CKM.4 Cryptographic key destruction • FCS_COP.1 Cryptographic operation • FPR_UNO.1 Unobservability • FCS_RNG.1 Random number generation • FCS_COP.1/DRBG Cryptographic operation
SF.PIN	<p>The TOE implements secure PIN compare functions and integrity protection of the PIN.</p> <p>This TSF enforces the following SFRs:</p> <ul style="list-style-type: none"> • FPR_UNO.1 Unobservability • FDP_SDI.2 Stored data integrity monitoring and action

8.1.2 eUICC

SF.eUICC_CRYPTO	<p>This TSF provides key creation, key management, key deletion and cryptographic functionality specific to the eUICC component.</p> <p>It provides the API in accordance to eUICC specification [SGP.02].</p> <p>This TSF also enforces protection of key material during cryptographic functions processing and key Generation, against state-of-the-art attacks, including IC power consumption analysis.</p> <p>The TSF also provides a secure random generator. This number is used to provide functionality to Platform Support Functions, like generation of a random challenge and generation of a shared secret implemented in FDP_ACF.1/ECASD.</p> <p>This TSF enforces the following SFRs:</p> <ul style="list-style-type: none"> • FPT_EMS.1 • FCS_CKM.1/SCP-SM • FCS_CKM.2/SCP-MNO • FCS_CKM.2/Mobile_network • FCS_CKM.4/SCP-SM • FCS_CKM.4/SCP-MNO • FCS_CKM.4/Mobile_network • FCS_COP.1/Mobile_network • FCS_RNG.1 • FCS_COP.1/DRBG
SF.eUICC_ACCESS	<p>This TSF handles the access to eUICC features by external or local users. It based on JavaCard and GlobalPlatform features to implement:</p> <ul style="list-style-type: none"> • Flow controls. • Access control • Identification and authentication of users. • Establishment of trusted channels in accordance to eUICC specifications [SGP.02]. <p>This TSF enforces the following SFRs:</p> <ul style="list-style-type: none"> • FDP_IFC.1/SCP • FDP_IFF.1/SCP • FDP_IFC.1/Platform_services • FDP_IFF.1/Platform_services • FPT_FLS.1/Platform_services • FDP_ACC.1/ISDR • FDP_ACF.1/ISDR • FDP_ACC.1/ECASD • FDP_ACC.1/ISDP

	<ul style="list-style-type: none"> • FDP_ACF.1/ECASD • FDP_ACF.1/ISDP • FMT_MSA.1/PSF_DATA • FMT_MSA.1/POL1 • FMT_MSA.1/CERT_KEYS • FMT_SMF.1/EUICC • FMT_SMR.1/EUICC • FMT_MSA.3/eUICC • FIA_UID.1/EXT • FIA_UAU.1/EXT • FIA_UAU.4/EXT • FIA_USB.1/EXT • FIA_UID.1/MNO-SD • FIA_USB.1/MNO-SD • FIA_ATD.1/eUICC • FIA_API.1/eUICC • FTP_ITC.1/SCP • FDP_ITC.2/SCP • FPT_TDC.1/SCP • FDP_UCT.1/SCP • FDP_UIT.1/SCP
<p>SF.eUICC_PROTECTION</p>	<p>This TSF extends the scope of self-protections features provided by the Java Card platform to the eUICC component needs.</p> <p>This TSF enforces the following SFRs:</p> <ul style="list-style-type: none"> • FDP_SDI.1/EUICC • FDP_RIP.1/EUICC • FPT_FLS.1/EUICC

9 Rationales

9.1 Security Requirements Rationale

9.1.1 Java Card

9.1.1.1 Objectives

9.1.1.1.1 Security Objectives for the TOE

Objective	Rationale
O.SID	<p>Subjects' identity is AID-based (applets, packages and CAP files), and is met by the following SFRs: FDP_ITC.2/Installer, FIA_ATD.1/AID, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_MSA.1/ADEL, FMT_MSA.1/CM, FMT_MSA.3/ADEL, FMT_MSA.3/FIREWALL, FMT_MSA.3/JCVM, FMT_MSA.3/CM, FMT_SMF.1/CM, FMT_SMF.1/ADEL, FMT_SMF.1/ADEL, FMT_MTD.1/JCRE and FMT_MTD.3/JCRE.</p> <p>Installation procedures ensure protection against forgery (the AID of an applet is under the control of the TSFs) or re-use of identities (FIA_UID.2/AID, FIA_USB.1/AID).</p>
O.FIREWALL	<p>This objective is met by the FIREWALL access control policy FDP_ACC.2/FIREWALL and FDP_ACF.1/FIREWALL, the JCVM information flow control policy (FDP_IFF.1/JCVM, FDP_IFC.1/JCVM) and the functional requirement FDP_ITC.2/Installer.</p> <p>The functional requirements of the class FMT (FMT_MTD.1/JCRE, FMT_MTD.3/JCRE, FMT_SMR.1/Installer, FMT_SMR.1, FMT_SMF.1, FMT_SMR.1/ADEL, FMT_SMF.1/ADEL, FMT_SMF.1/CM, FMT_MSA.1/CM, FMT_MSA.3/CM, FMT_SMR.1/CM, FMT_MSA.2/FIREWALL_JCVM, FMT_MSA.3/FIREWALL, FMT_MSA.3/JCVM, FMT_MSA.1/ADEL, FMT_MSA.3/ADEL, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM) also indirectly contribute to meet this objective.</p>
O.GLOBAL_ARRAYS_CONFID	<p>Only arrays can be designated as global, and the only global arrays required in the Java Card API are the APDU buffer, the global byte array input parameter (bArray) to an applet's install method and the global arrays created by the JCSYSTEM.makeGlobalArray(...) method. The clearing requirement of these arrays is met by (FDP_RIP.1/APDU, FDP_RIP.1/GlobalArray and FDP_RIP.1/bArray respectively). The JCVM information flow control policy (FDP_IFF.1/JCVM, FDP_IFC.1/JCVM) prevents an application from keeping a pointer to a shared buffer, which could be used to read its contents when the buffer is being used by another application.</p>
O.GLOBAL_ARRAYS_INTEG	<p>This objective is met by the JCVM information flow control policy (FDP_IFF.1/JCVM, FDP_IFC.1/JCVM), which prevents an application from keeping a pointer to the APDU buffer of the card, to the global byte array of the applet's install method or to the global arrays created by the JCSYSTEM.makeGlobalArray(...) method. Such a pointer could be used to access and modify it when the buffer is being used by another application.</p>
O.ARRAY_VIEWS_CONFID	<p>Array views have security attributes of temporary objects where the JCVM information flow control policy (FDP_IFF.1/JCVM, FDP_IFC.1/JCVM) prevents an application from storing a reference to the array view. Furthermore, array views may not have ATTR_READABLE_VIEW security attribute which ensures that no application can read the contents of the array view.</p>
O.ARRAY_VIEWS_INTEG	<p>Array views have security attributes of temporary objects where the JCVM information flow control policy (FDP_IFF.1/JCVM, FDP_IFC.1/JCVM) prevents an application from storing a reference to the array view. Furthermore, array views may not have ATTR_WRITABLE_VIEW security attribute which ensures that no application can alter the contents of the array view.</p>
O.NATIVE	<p>This security objective is covered by FDP_ACF.1/FIREWALL: the only means to execute native code is the invocation of a Java Card API method. This objective mainly relies on the environmental objective OE.CAP_FILE, which uphold the assumption A.CAP_FILE.</p>

Objective	Rationale
O.OPERATE	<p>The TOE is protected in various ways against applets' actions (FPT_TDC.1), the FIREWALL access control policy FDP_ACC.2/FIREWALL and FDP_ACF.1/FIREWALL, and is able to detect and block various failures or security violations during usual working (FPT_FLS.1/ADEL, FPT_FLS.1, FPT_FLS.1/ODEL, FPT_FLS.1/Installer, FAU_ARP.1). Its security-critical parts and procedures are also protected: safe recovery from failure is ensured (FPT_RCV.3/Installer), applets' installation may be cleanly aborted (FDP_ROL.1/FIREWALL), communication with external users and their internal subjects is well-controlled (FDP_ITC.2/Installer, FIA_ATD.1/AID, FIA_USB.1/AID) to prevent alteration of TSF data (also protected by components of the FPT class).</p> <p>Almost every objective and/or functional requirement indirectly contributes to this one too.</p> <p>Application note: Startup of the TOE (TSF-testing) can be covered by FPT_TST.1. This SFR component is not mandatory in [JCRE], but appears in most of security requirements documents for masked applications. Testing could also occur randomly. Self-tests may become mandatory in order to comply with FIPS certification [FIPS 140-2].</p>
O.REALLOCATION	<p>This security objective is satisfied by the following SFRs: FDP_RIP.1/APDU, FDP_RIP.1/GlobalArray, FDP_RIP.1/bArray, FDP_RIP.1/ABORT, FDP_RIP.1/KEYS, FDP_RIP.1/TRANSIENT, FDP_RIP.1/ODEL, FDP_RIP.1/OBJECTS, FDP_RIP.1/ADEL, which imposes that the contents of the re-allocated block shall always be cleared before delivering the block.</p>
O.RESOURCES	<p>The TSFs detects stack/memory overflows during execution of applications (FAU_ARP.1, FPT_FLS.1/ADEL, FPT_FLS.1, FPT_FLS.1/ODEL, FPT_FLS.1/Installer). Failed installations are not to create memory leaks (FDP_ROL.1/FIREWALL, FPT_RCV.3/Installer) as well. Memory management is controlled by the TSF (FMT_MTD.1/JCRE, FMT_MTD.3/JCRE, FMT_SMR.1/Installer, FMT_SMR.1, FMT_SMF.1 FMT_SMR.1/ADEL, FMT_SMF.1/ADEL, FMT_SMF.1/CM and FMT_SMR.1/CM).</p> <p>Additionally, if the TOE provides JCRMI functionality, memory management is controlled by the TSF FMT_SMR.1/JCRMI, and FMT_SMF.1/JCRMI.</p>
O.ALARM	<p>This security objective is met by FPT_FLS.1/Installer, FPT_FLS.1, FPT_FLS.1/ADEL, FPT_FLS.1/ODEL which guarantee that a secure state is preserved by the TSF when failures occur, and FAU_ARP.1 which defines TSF reaction upon detection of a potential security violation.</p>
O.CIPHER	<p>This security objective is directly covered by FCS_CKM.1, FCS_CKM.4 and FCS_COP.1. The SFR FPR_UNO.1 contributes in covering this security objective and controls the observation of the cryptographic operations which may be used to disclose the keys.</p>
O.RNG	<p>This security objective is directly covered by FCS_RNG.1 and FCS_COP.1/DRBG which ensure the cryptographic quality of random number generation.</p>
O.KEY-MNGT	<p>This relies on the same security functional requirements as O.CIPHER, plus FDP_RIP.1 and FDP_SDI.2/DATA as well. Precisely it is met by the following components: FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FPR_UNO.1, FDP_RIP.1/ODEL, FDP_RIP.1/OBJECTS, FDP_RIP.1/APDU, FDP_RIP.1/GlobalArray FDP_RIP.1/bArray, FDP_RIP.1/ABORT, FDP_RIP.1/KEYS, FDP_RIP.1/ADEL and FDP_RIP.1/TRANSIENT.</p>
O.PIN-MNGT	<p>This security objective is ensured by FDP_RIP.1/ODEL, FDP_RIP.1/OBJECTS, FDP_RIP.1/APDU, FDP_RIP.1/GlobalArray FDP_RIP.1/bArray, FDP_RIP.1/ABORT, FDP_RIP.1/KEYS, FDP_RIP.1/ADEL, FDP_RIP.1/TRANSIENT, FPR_UNO.1, FDP_ROL.1/FIREWALL and FDP_SDI.2/DATA security functional requirements. The TSFs behind these are implemented by API classes. The firewall security functions FDP_ACC.2/FIREWALL and FDP_ACF.1/FIREWALL shall protect the access to private and internal data of the objects.</p>
O.TRANSACTION	<p>Directly met by FDP_ROL.1/FIREWALL, FDP_RIP.1/ABORT, FDP_RIP.1/ODEL, FDP_RIP.1/APDU, FDP_RIP.1/GlobalArray FDP_RIP.1/bArray, FDP_RIP.1/KEYS, FDP_RIP.1/ADEL, FDP_RIP.1/TRANSIENT and FDP_RIP.1/OBJECTS (more precisely, by the element FDP_RIP.1.1/ABORT).</p>
O.OBJ-DELETION	<p>This security objective specifies that deletion of objects is secure. The security objective is met by the security functional requirements FDP_RIP.1/ODEL and FPT_FLS.1/ODEL.</p>

Objective	Rationale
O.DELETION	This security objective specifies that applet and CAP file deletion must be secure. The non-introduction of security holes is ensured by the ADEL access control policy (FDP_ACC.2/ADEL, FDP_ACF.1/ADEL). The integrity and confidentiality of data that does not belong to the deleted applet or CAP file is a by-product of this policy as well. Non-accessibility of deleted data is met by FDP_RIP.1/ADEL and the TSFs are protected against possible failures of the deletion procedures (FPT_FLS.1/ADEL, FPT_RCV.3/Installer). The security functional requirements of the class FMT (FMT_MSA.1/ADEL, FMT_MSA.3/ADEL, FMT_SMR.1/ADEL) included in the group ADELG also contribute to meet this objective.
O.LOAD	This security objective specifies that the loading of a CAP file into the card must be secure. Evidence of the origin of the CAP file is enforced (FCO_NRO.2/CM) and the integrity of the corresponding data is under the control of the CAP FILE LOADING information flow policy (FDP_IFC.2/CM, FDP_IFF.1/CM) and FDP_UIT.1/CM. Appropriate identification (FIA_UID.1/CM) and transmission mechanisms are also enforced (FTP_ITC.1/CM).
O.INSTALL	This security objective specifies that installation of applets must be secure. Security attributes of installed data are under the control of the FIREWALL access control policy (FDP_ITC.2/Installer), and the TSFs are protected against possible failures of the installer (FPT_FLS.1/Installer, FPT_RCV.3/Installer).
O.CARD-MANAGEMENT	<p>This objective is fulfilled by the following set of SFR:</p> <p>FDP_ACC.2/ADEL and FDP_ACF.1/ADEL contribute to meet the objective by the ADEL access control policy which ensures the non-introduction of security holes.</p> <p>FDP_RIP.1/ADEL ensures the non-accessibility of deleted data.</p> <p>FMT_MSA.1/ADEL and FMT_MSA.3/ADEL enforce the ADEL access control SFP.</p> <p>FMT_SMR.1/ADEL maintains the role applet deletion manager.</p> <p>FPT_RCV.3/Installer protects the TSFs against possible failures of the deletion procedures.</p> <p>FPT_FLS.1/Installer protects the TSFs against possible failures of the installer.</p> <p>FPT_FLS.1/ADEL protects the TSFs against possible failures of the deletion procedures.</p> <p>FDP_UIT.1/CM enforces the Secure Channel Protocol information flow control policy and the Security Domain access control policy which controls the integrity of the corresponding data.</p> <p>FDP_IFF.1/CM ensures the access control policy for the loaded data (as packages).</p> <p>The FCO_NRO.2/CM ensures the origin of the load file. It verifies the identity of the origin of the load file before start the loading</p> <p>FDP_IFC.2/CM ensures that loading commands are issued in the Secure Channel session.</p> <p>FDP_ROL.1/Firewall ensures that the card management operations are cleaned aborted</p> <p>FDP_ITC.2/Installer enforces the Firewall access control policy and flow control policy when importing card management data.</p> <p>FPT_FLS.1/ODEL ensures the preservation of secure state when failures occur.</p> <p>FMT_MSA.1/CM ensures the management of the security attributes to the card manager, for the modification of the defined security attributes.</p> <p>FMT_MSA.3/CM ensures that the security attributes can only be changed by the card manager.</p> <p>FMT_SMF.1/CM allows only the card manger to modify the security attributes of the management functions. The security role is specified in the FMT_SMR.1/CM.</p> <p>FTP_ITC.1/CM ensures the trusted Channel Communications.</p> <p>FPR_UNO.1 ensures the un-observability of the CM key when imported..</p> <p>FPT_TST.1 ensures the correct operation of the card management functions as it tests the integrity of the TSF functions during initial start-up.</p>
O.SCP.RECOVERY	<p>FPT_RCV.3/Installer is used to assist the TOE to recover in the event of a power failure. The component FAU_ARP.1 is used to ensure the reinitialization of the Java Card System and its data after card tearing and power failure. The component FPT_FLS.1 is used to preserve a secure state after failure.</p> <p>O.SCP.SUPPORT</p>
O.SCP.SUPPORT	All crypto SFRs supports this objective as they provide the functionality to the Java Card and Global Platform (FCS_CKM.1, FCS_CKM.4, FCS_COP.1)

Objective	Rationale
	All the FSRs related to the Firewall contribute to the realization of the objective (FDP_ROL.1/FIREWALL).
O.SCP.IC	This objective is met by providing physical protection (FPR_UNO.1, FPT_EMS.1 and FPT_PHP.3) and taking action upon security violation (FAU_ARP.1).

9.1.1.2 Rationale tables of Security Objectives and SFRs

Objective	SFR mapping
O.SID	FIA_ATD.1/AID, FIA_UID.2/AID, FMT_MSA.1/JCRE, FMT_MSA.1/ADEL, FMT_MSA.3/ADEL, FMT_MSA.3/FIREWALL, FMT_MSA.1/CM, FMT_MSA.3/CM, FDP_ITC.2/Installer, FMT_SMF.1/CM, FMT_SMF.1/ADEL, FMT_MTD.1/JCRE, FMT_MTD.3/JCRE, FIA_USB.1/AID, FMT_MSA.1/JCVM, FMT_MSA.3/JCVM
O.FIREWALL	FDP_IFC.1/JCVM, FDP_IFF.1/JCVM, FMT_SMR.1/Installer, FMT_MSA.1/CM, FMT_MSA.3/CM, FMT_SMR.1/CM, FMT_MSA.3/FIREWALL, FMT_SMR.1, FMT_MSA.1/ADEL, FMT_MSA.3/ADEL, FMT_SMR.1/ADEL, FMT_MSA.1/JCRE, FDP_ITC.2/Installer, FDP_ACC.2/FIREWALL, FDP_ACF.1/FIREWALL, FMT_SMF.1/ADEL, FMT_SMF.1/CM, FMT_SMF.1, FMT_MSA.2/FIREWALL_JCVM, FMT_MTD.1/JCRE, FMT_MTD.3/JCRE, FMT_MSA.1/JCVM, FMT_MSA.3/JCVM
O.GLOBAL_ARRAYS_CONFID	FDP_IFC.1/JCVM, FDP_IFF.1/JCVM, FDP_RIP.1/bArray, FDP_RIP.1/APDU, FDP_RIP.1/GlobalArray, FDP_RIP.1/ODEL, FDP_RIP.1/OBJECTS, FDP_RIP.1/ABORT, FDP_RIP.1/KEYS, FDP_RIP.1/ADEL, FDP_RIP.1/TRANSIENT
O.GLOBAL_ARRAYS_INTEG	FDP_IFC.1/JCVM, FDP_IFF.1/JCVM
O.ARRAY_VIEWS_CONFID	FDP_IFC.1/JCVM, FDP_IFF.1/JCVM, FDP_ACC.2/Firewall, FDP_ACF.1/Firewall
O.ARRAY_VIEWS_INTEG	FDP_IFC.1/JCVM, FDP_IFF.1/JCVM, FDP_ACC.2/Firewall, FDP_ACF.1/Firewall
O.NATIVE	FDP_ACF.1/FIREWALL
O.OPERATE	FAU_ARP.1, FDP_ROL.1/FIREWALL, FIA_ATD.1/AID, FPT_FLS.1/ADEL, FPT_FLS.1, FPT_FLS.1/ODEL, FPT_FLS.1/Installer, FDP_ITC.2/Installer, FPT_RCV.3/Installer, FDP_ACC.2/FIREWALL, FDP_ACF.1/FIREWALL, FPT_TDC.1, FIA_USB.1/AID
O.REALLOCATION	FDP_RIP.1/ABORT, FDP_RIP.1/APDU, FDP_RIP.1/GlobalArray, FDP_RIP.1/bArray, FDP_RIP.1/KEYS, FDP_RIP.1/TRANSIENT, FDP_RIP.1/ADEL, FDP_RIP.1/ODEL, FDP_RIP.1/OBJECTS
O.RESOURCES	FAU_ARP.1, FDP_ROL.1/FIREWALL, FMT_SMR.1/Installer, FMT_SMR.1, FMT_SMR.1/ADEL, FPT_FLS.1/Installer, FPT_FLS.1/ODEL, FPT_FLS.1, FPT_FLS.1/ADEL, FPT_RCV.3/Installer, FMT_SMR.1/CM, FMT_SMF.1/ADEL, FMT_SMF.1/CM, FMT_SMF.1, FMT_MTD.1/JCRE, FMT_MTD.3/JCRE
O.ALARM	FPT_FLS.1/Installer, FPT_FLS.1, FPT_FLS.1/ADEL, FPT_FLS.1/ODEL, FAU_ARP.1
O.CIPHER	FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FPR_UNO.1
O.RNG	FCS_RNG.1, FCS_COP.1/DRBG
O.KEY-MNGT	FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FPR_UNO.1, FDP_RIP.1/ODEL, FDP_RIP.1/OBJECTS, FDP_RIP.1/APDU, FDP_RIP.1/GlobalArray, FDP_RIP.1/bArray, FDP_RIP.1/ABORT, FDP_RIP.1/KEYS, FDP_SDI.2/DATA, FDP_RIP.1/ADEL, FDP_RIP.1/TRANSIENT
O.PIN-MNGT	FDP_RIP.1/ODEL, FDP_RIP.1/OBJECTS, FDP_RIP.1/APDU, FDP_RIP.1/GlobalArray, FDP_RIP.1/bArray, FDP_RIP.1/ABORT, FDP_RIP.1/KEYS, FPR_UNO.1, FDP_RIP.1/ADEL, FDP_RIP.1/TRANSIENT, FDP_ROL.1/FIREWALL, FDP_SDI.2/DATA, FDP_ACC.2/FIREWALL, FDP_ACF.1/FIREWALL
O.TRANSACTION	FDP_ROL.1/FIREWALL, FDP_RIP.1/ABORT, FDP_RIP.1/ODEL, FDP_RIP.1/APDU, FDP_RIP.1/GlobalArray, FDP_RIP.1/bArray, FDP_RIP.1/KEYS, FDP_RIP.1/ADEL, FDP_RIP.1/TRANSIENT, FDP_RIP.1/OBJECTS
O.OBJ-DELETION	FDP_RIP.1/ODEL, FPT_FLS.1/ODEL
O.DELETION	FDP_ACC.2/ADEL, FDP_ACF.1/ADEL, FDP_RIP.1/ADEL, FPT_FLS.1/ADEL, FPT_RCV.3/Installer, FMT_MSA.1/ADEL, FMT_MSA.3/ADEL, FMT_SMR.1/ADEL

Objective	SFR mapping
O.LOAD	FCO_NRO.2/CM, FDP_IFC.2/CM, FDP_IFF.1/CM, FDP_UIT.1/CM, FIA_UID.1/CM, FTP_ITC.1/CM
O.INSTALL	FDP_ITC.2/Installer, FPT_RCV.3/Installer, FPT_FLS.1/Installer
O.CARD-MANAGEMENT	FDP_ACC.2/ADEL, FDP_ACF.1/ADEL, FDP_RIP.1/ADEL, FMT_MSA.1/ADEL, FMT_MSA.3/ADEL, FMT_SMR.1/ADEL, FPT_RCV.3/Installer, FPT_FLS.1/Installer, FPT_FLS.1/ADEL, FDP_UIT.1/CM, FDP_IFF.1/CM, FCO_NRO.2/CM, FDP_IFC.2/CM, FDP_ROL.1/Firewall, FDP_ITC.2/Installer, FPT_FLS.1/ODEL, FMT_MSA.1/CM, FMT_MSA.3/CM, FMT_SMF.1/CM, FMT_SMR.1/CM, FTP_ITC.1/CM, FPR_UNO.1, FPT_TST.1
O.SCP.RECOVERY	FPT_RCV.3/Installer, FAU_ARP.1, FPT_FLS.1
O.SCP.SUPPORT	FCS_CKM.1, FCS_CKM.4, FCS_COP.1, FDP_ROL.1/FIREWALL
O.SCP.IC	FPR_UNO.1, FPT_EMS.1, FPT_PHP.3, FAU_ARP.1.

9.1.1.3 Dependencies

9.1.1.4 SFR Dependencies

Requirement	Dependency	Satisfied by
FDP_ACC.2/FIREWALL	(FDP_ACF.1)	FDP_ACF.1/FIREWALL
FDP_ACF.1/FIREWALL	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.2/FIREWALL, FMT_MSA.3/FIREWALL
FDP_IFC.1/JCVM	(FDP_IFF.1)	FDP_IFF.1/JCVM
FDP_IFF.1/JCVM	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/JCVM, FMT_MSA.3/JCVM
FDP_RIP.1/OBJECTS	No Dependencies	
FMT_MSA.1/JCRE	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.2/FIREWALL, FMT_SMR.1
FMT_MSA.1/JCVM	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.2/FIREWALL, FDP_IFC.1/JCVM, FMT_SMF.1, FMT_SMR.1
FMT_MSA.2/FIREWALL_JCVM	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.1) and (FMT_SMR.1)	FDP_ACC.2/FIREWALL, FDP_IFC.1/JCVM, FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_SMR.1
FMT_MSA.3/FIREWALL	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/JCRE, FMT_MSA.1/JCVM, FMT_SMR.1
FMT_MSA.3/JCVM	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/JCVM, FMT_SMR.1
FMT_SMF.1	No Dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.2/AID
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_COP.1, FCS_CKM.4
FCS_CKM.4	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1
FCS_COP.1	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_CKM.1, FCS_CKM.4
FCS_RNG.1	No Dependencies	
FDP_RIP.1/ABORT	No Dependencies	
FDP_RIP.1/APDU	No Dependencies	
FDP_RIP.1/bArray	No Dependencies	
FDP_RIP.1/GlobalArray	No Dependencies	

FDP_RIP.1/KEYS	No Dependencies	
FDP_RIP.1/TRANSIENT	No Dependencies	
FDP_ROL.1/FIREWALL	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.2/FIREWALL, FDP_IFC.1/JCVM
FAU_ARP.1	(FAU_SAA.1)	
FDP_SDI.2/DATA	No Dependencies	
FPR_UNO.1	No Dependencies	
FPT_FLS.1	No Dependencies	
FPT_TDC.1	No Dependencies	
FIA_ATD.1/AID	No Dependencies	
FIA_UID.2/AID	No Dependencies	
FIA_USB.1/AID	(FIA_ATD.1)	FIA_ATD.1/AID
FMT_MTD.1/JCRE	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMF.1, FMT_SMR.1
FMT_MTD.3/JCRE	(FMT_MTD.1)	FMT_MTD.1/JCRE
FDP_ITC.2/Installer	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/CM, FTP_ITC.1/CM, FPT_TDC.1
FMT_SMR.1/Installer	(FIA_UID.1)	
FPT_FLS.1/Installer	No Dependencies	
FPT_RCV.3/Installer	(AGD_OPE.1)	AGD_OPE.1
FDP_ACC.2/ADEL	(FDP_ACF.1)	FDP_ACF.1/ADEL
FDP_ACF.1/ADEL	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.2/ADEL, FMT_MSA.3/ADEL
FDP_RIP.1/ADEL	No Dependencies	
FMT_MSA.1/ADEL	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.2/ADEL, FMT_SMF.1/ADEL, FMT_SMR.1/ADEL
FMT_MSA.3/ADEL	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/ADEL, FMT_SMR.1/ADEL
FMT_SMF.1/ADEL	No Dependencies	
FMT_SMR.1/ADEL	(FIA_UID.1)	
FPT_FLS.1/ADEL	No Dependencies	
FDP_RIP.1/ODEL	No Dependencies	
FPT_FLS.1/ODEL	No Dependencies	
FCO_NRO.2/CM	(FIA_UID.1)	FIA_UID.1/CM
FDP_IFC.2/CM	(FDP_IFF.1)	FDP_IFF.1/CM
FDP_IFF.1/CM	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.2/CM, FMT_MSA.3/CM
FDP_UIT.1/CM	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.2/CM, FTP_ITC.1/CM
FIA_UID.1/CM	No Dependencies	
FMT_MSA.1/CM	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_IFC.2/CM, FMT_SMF.1/CM, FMT_SMR.1/CM
FMT_MSA.3/CM	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/CM, FMT_SMR.1/CM
FMT_SMF.1/CM	No Dependencies	
FMT_SMR.1/CM	(FIA_UID.1)	FIA_UID.1/CM
FTP_ITC.1/CM	No Dependencies	

Rationale for the exclusion of dependencies:

- The dependency FIA_UID.1 of FMT_SMR.1/Installer is discarded. The Java Card PP [PP-JC] does not require the identification of the "installer" since it can be considered as part of the TSF.
- The dependency FIA_UID.1 of FMT_SMR.1/ADEL is discarded. The Java Card PP [PP-JC] does not require the identification of the "deletion manager" since it can be considered as part of the TSF.
- The dependency FMT_SMF.1 of FMT_MSA.1/JCRE is discarded. The dependency between FMT_MSA.1/JCRE and FMT_SMF.1 is not satisfied because no management functions are required for the Java Card RE.
- The dependency FAU_SAA.1 of FAU_ARP.1 is discarded. The dependency of FAU_ARP.1 on FAU_SAA.1 assumes that a "potential security violation" generates an audit event. On the contrary, the events listed in FAU_ARP.1 are self-contained (arithmetic exception, ill-formed bytecodes, access failure) and ask for a straightforward reaction of the TSFs on their occurrence at runtime. The JVM or other components of the TOE detect these events during their usual working order. Thus, there is no mandatory audit recording in the Java Card PP [PP-JC].

9.1.1.5 SARs Dependency Rationale

This rationale shows that all dependencies of all security requirements have been addressed:

Requirement	Dependency	Satisfied by
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 11 SFR dependencies rationale

9.1.1.5.1 Rationale for the Security Assurance Requirements

EAL4 is required for this type of TOE and product since it is intended to defend against sophisticated attacks. This evaluation assurance level allows a developer to gain maximum assurance from positive security engineering based on good practices. EAL4 represents the highest practical level of assurance expected for a commercial grade product. In order to provide a meaningful level of assurance that the TOE and its embedding product provide an adequate level of defense against such attacks: the evaluators should have access to the low level design and source code. The lowest for which such access is required is EAL4.

9.1.1.5.2 ALC_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE and the embedding product. The standard ALC_DVS.1 requirement mandated by EAL4 is not enough. Due to the nature of the TOE and embedding product, it is necessary to justify the sufficiency of these procedures to protect their confidentiality and integrity. ALC_DVS.2 has no dependencies.

9.1.1.5.3 AVA_VAN.5 Advanced methodical vulnerability analysis

The TOE is intended to operate in hostile environments. AVA_VAN.5 "Advanced methodical vulnerability analysis" is considered as the expected level for Java Card technology-based products hosting sensitive applications. AVA_VAN.5 has dependencies on ADV_ARC.1, ADV_FSP.1, ADV_TDS.3, ADV_IMP.1, AGD_PRE.1 and AGD_OPE.1. All of them are satisfied by EAL4.

9.1.2 eUICC

This rationale shows that all security objectives for the TOE are upheld by the security functional requirements.

9.1.2.1 Objectives

9.1.2.1.1 Security Objectives for the TOE

Objective	Rationale
O.PSF	<p>All SFRs related to Security Domains (FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FDP_ACC.1/ISDP, FDP_ACF.1/ISDP, FDP_ACC.1/ECASD and FDP_ACF.1/ECASD) cover this security objective by enforcing a Security Domain access control policy (rules and restrictions) that meets the card content management rules.</p> <p>FMT_MSA.1/POL1 supports these SFRs by ensuring management of the POL1 policy file, which ensures that lifecycle modifications are made according to the authorized policy.</p> <p>FMT_MSA.1/PSF_DATA restricts the state transitions that can apply to PSF data (ISD-P state and Fallback attribute) that are used as security attributes by other security policies of the TSF (ISD-R access control SFP and ISD-P access control SFP).</p> <p>The objective also requires a secure failure mode as described in FPT_FLS.1.</p> <p>FCS_RNG.1 and FCS_COP.1/DRBG are required to support FDP_ACF.1/ECASD.</p>
O.eUICC-DOMAIN-RIGHTS	<p>The requirements FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FDP_ACC.1/ISDP, FDP_ACF.1/ISDP, FDP_ACC.1/ECASD and FDP_ACF.1/ECASD ensure that ISD-R, ISD-P, MNO-SD and ECASD functionality and content are only accessible to the corresponding authenticated user. FTP_ITC.1/SCP provide the corresponding secure channels to the authorized users.</p> <p>FMT_MSA.1/POL1, FMT_MSA.1/PSF_DATA, FMT_MSA.1/CERT_KEYS and FMT_MSA.3 address the management of the security attributes used by the SFP.</p> <p>FCS_RNG.1 and FCS_COP.1/DRBG are required to support FDP_ACF.1/ECASD.</p> <p>NB: there is no secure channel to access ECASD, since its services can be accessed by on-card actors, but its content cannot be modified during the lifecycle of the eUICC.</p>
O.SECURE-CHANNELS	<p>The requirements FTP_ITC.1/SCP, FPT_TDC.1/SCP, FDP_UCT.1/SCP, FDP_UIT.1/SCP, FDP_ITC.2/SCP, FDP_IFC.1/SCP, FDP_IFF.1/SCP, cover this security objective by enforcing Secure Channel Protocol information flow control SFP that ensures that transmitted commands and data are protected from unauthorized disclosure and modification. They rely on FCS_CKM.1/SCP-SM, FCS_CKM.2/SCP-MNO, FCS_CKM.4/SCP-SM and FCS_CKM.4/SCP-MNO for key management.</p> <p>Identification and authentication SFRs (FIA_UID.1/EXT, FIA_UAU.1/EXT, FIA_UAU.4/EXT, FIA_UID.1/MNO-SD, FIA_USB.1/MNO-SD, FIA_USB.1/EXT) support this security objective by requiring authentication and identification from the distant SM-DP, SM-SR and MNO OTA Platform in order to establish these secure channels.</p> <p>FIA_ATD.1, FMT_MSA.1/CERT_KEYS and FMT_MSA.3 address the management of the security attributes used by the SFP.</p> <p>FMT_SMF.1 and FMT_SMR.1 support these SFRs by providing management of roles and management of functions.</p>
O.INTERNAL-SECURECHANNELS	<p>FPT_EMS.1 ensures that secret data stored or transmitted within the TOE shall not be disclosed in cases of side channel attacks. This includes in particular the shared secrets transmitted between ECASD and ISD-R/ISD-P.</p> <p>FDP_SDI.1 ensures that the shared secret cannot be modified during this transmission.</p> <p>FDP_RIP.1 ensures that the shared secret cannot be recovered from deallocated resources.</p>
O.PROOF_OF_IDENTITY	<p>This objective is covered by the extended requirement FIA_API.1.</p>

Objective	Rationale
O.OPERATE	FPT_FLS.1/Platform_services requires that failures do not impact on the security of the TOE.
O.API	FDP_IFC.1/Platform_services, FDP_IFF.1/Platform_services, FMT_MSA.3 and FMT_SMR.1 and FMT_SMF.1 state the policy for controlling the access to TOE services and resources by the Application Layer ("API information flow control policy"). Atomicity is provided by the FPT_FLS.1/Platform_services requirement.
O.DATACONFIDENTIALITY	FDP_UCT.1/SCP addresses the reception of data from off-card actors, while the access control SFPs (FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FDP_ACC.1/ECASD) address the isolation between Security Domains. FPT_EMS.1 ensures that secret data stored or transmitted within the TOE shall not be disclosed in cases of side channel attacks. FDP_RIP.1 ensures that no residual confidential data is available. FCS_COP.1/Mobile_network, FCS_CKM.2/Mobile_network and FCS_CKM.4/Mobile_network address the cryptographic algorithms present in the Telecom Framework, the distribution and the destruction of associated keys.
O.DATA-INTEGRITY	FDP_UIT.1/SCP addresses the reception of data from off-card actors, while the access control SFPs (FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FDP_ACC.1/ECASD) address the isolation between Security Domains. FDP_SDI.1 specifies the Profile data that is monitored in case of an integrity breach (for example modification of the received profile during the installation operation).
O.ALGORITHMS	The algorithms are defined in FCS_COP.1/Mobile_network. FCS_CKM.2/Mobile_network describes how the keys are distributed within the MNO profiles, and FCS_CKM.4/Mobile_network describes the destruction of the keys.

9.1.2.2 Rationale tables of Security Objectives and SFRs

Objective	SFR mapping
O.PSF	FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FDP_ACC.1/ISDP, FDP_ACF.1/ISDP, FDP_ACC.1/ECASD, FDP_ACF.1/ECASD, FMT_MSA.1/PSF_DATA, FMT_MSA.1/POL1, FPT_FLS.1, FCS_RNG.1, FCS_COP.1/DRBG
O.eUICC-DOMAIN-RIGHTS	FDP_ACC.1/ISDR, FDP_ACF.1/ISDR, FDP_ACC.1/ISDP, FDP_ACF.1/ISDP, FDP_ACC.1/ECASD, FDP_ACF.1/ECASD, FTP_ITC.1/SCP, FMT_MSA.1/PSF_DATA, FMT_MSA.1/POL1, FMT_MSA.1/CERT_KEYS, FMT_MSA.3, FCS_RNG.1, FCS_COP.1/DRBG
O.SECURE-CHANNELS	FTP_ITC.1/SCP, FPT_TDC.1/SCP, FDP_UCT.1/SCP, FDP_UIT.1/SCP, FDP_ITC.2/SCP, FDP_IFC.1/SCP, FDP_IFF.1/SCP, FCS_CKM.1/SCP-SM, FCS_CKM.2/SCP-MNO, FCS_CKM.4/SCP-SM, FCS_CKM.4/SCP-MNO, FIA_UID.1/EXT, FIA_UAU.1/EXT, FIA_UAU.4/EXT, FIA_UID.1/MNO-SD, FIA_USB.1/MNO-SD, FIA_USB.1/EXT, FIA_ATD.1, FMT_MSA.1/CERT_KEYS, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1
O.INTERNAL-SECURECHANNELS	FDP_RIP.1, FDP_SDI.1, FPT_EMS.1
O.PROOF_OF_IDENTITY	FIA_API.1
O.OPERATE	FPT_FLS.1/Platform_Services
O.API	FDP_IFC.1/Platform_services, FDP_IFF.1/Platform_services, FPT_FLS.1/Platform_Services, FMT_SMR.1, FMT_SMF.1, FMT_MSA.3
O.DATACONFIDENTIALITY	FDP_RIP.1, FDP_UCT.1/SCP, FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FDP_ACC.1/ECASD, FCS_COP.1/Mobile_network, FCS_CKM.4/Mobile_network, FCS_CKM.2/Mobile_network, FPT_EMS.1
O.DATA-INTEGRITY	FDP_UIT.1/SCP, FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FDP_ACC.1/ECASD, FDP_SDI.1
O.ALGORITHMS	FCS_COP.1/Mobile_network, FCS_CKM.4/Mobile_network, FCS_CKM.2/Mobile_network

9.1.2.3 Dependencies

9.1.2.4 SFR Dependencies

Requirement	Dependency	Satisfied by
FIA_UID.1/EXT	No Dependencies	
FIA_UAU.1/EXT	(FIA_UID.1)	FIA_UID.1/EXT
FIA_USB.1/EXT	(FIA_ATD.1)	FIA_ATD.1
FIA_UAU.4/EXT	No Dependencies	
FIA_UID.1/MNO-SD	No Dependencies	
FIA_USB.1/MNO-SD	(FIA_ATD.1)	FIA_ATD.1
FIA_ATD.1	No Dependencies	
FIA_API.1	No Dependencies	
FDP_IFC.1/SCP	(FDP_IFF.1)	FDP_IFF.1/SCP
FDP_IFF.1/SCP	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/SCP, FMT_MSA.3
FTP_ITC.1/SCP	No Dependencies	
FDP_ITC.2/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FPT_TDC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP, FPT_TDC.1/SCP
FPT_TDC.1/SCP	No Dependencies	
FDP_UCT.1/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP
FDP_UIT.1/SCP	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_IFC.1/SCP, FTP_ITC.1/SCP
FCS_CKM.1/SCP-SM	(FCS_CKM.2 or FCS_COP.1) and (FCS_CKM.4)	FCS_CKM.4/SCP-SM
FCS_CKM.2/SCP-MNO	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.1/SCP, FCS_CKM.4/SCP-MNO Rationale: This SFR is related to the distribution of <ul style="list-style-type: none"> D.MNO_KEYS during profile download Public keys distributed in the user certificates (CERT.SR.ECDSA and CERT.DP.ECDSA) or loaded pre issuance of the TOE (D.eUICC_CERT, D.CI_ROOT_PUBKEY) The distribution therefore requires a dependency to FDP_ITC.1/SCP, and secure destruction (FCS_CKM.4/SCP-MNO)
FCS_CKM.4/SCP-SM	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.1/SCP, FCS_CKM.1/SCP-SM Rationale: FCS_CKM.4/SCP-SM is related to the destruction of the following keys: <ul style="list-style-type: none"> Keys generated by the FCS_CKM.1/SCP-SM: <ul style="list-style-type: none"> D.ISDP_KEYS D.ISDR_KEYS Keys distributed by FDP_ITC.1/SCP: <ul style="list-style-type: none"> CERT.SR.ECDSA CERT.DP.ECDSA D.eUICC_CERT, D.eUICC_PRIVKEY,

		o D.CI_ROOT_PUBKEY,
FCS_CKM.4/SCP-MNO	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.1/SCP, FCS_CKM.1/SCP-SM
FCS_RNG.1	No Dependencies	
FCS_COP.1/DRBG	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FCS_RNG.1
FDP_ACC.1/ISDR	(FDP_ACF.1)	FDP_ACF.1/ISDR
FDP_ACF.1/ISDR	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ISDR, FMT_MSA.3
FDP_ACC.1/ISDP	(FDP_ACF.1)	FDP_ACF.1/ISDP
FDP_ACF.1/ISDP	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ISDP, FMT_MSA.3
FDP_ACC.1/ECASD	(FDP_ACF.1)	FDP_ACF.1/ECASD
FDP_ACF.1/ECASD	(FDP_ACC.1) and (FMT_MSA.3)	FDP_ACC.1/ECASD, FMT_MSA.3, FCS_RNG.1, FCS_COP.1/DRBG
FDP_IFC.1/Platform_services	(FDP_IFF.1)	FDP_IFF.1/Platform_services
FDP_IFF.1/Platform_services	(FDP_IFC.1) and (FMT_MSA.3)	FDP_IFC.1/Platform_services, FMT_MSA.3
FPT_FLS.1/Platform_Services	No Dependencies	
FPT_EMS.1	No Dependencies	
FDP_SDI.1	No Dependencies	
FDP_RIP.1	No Dependencies	
FPT_FLS.1	No Dependencies	
FMT_MSA.1/PSF_DATA	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FMT_SMF.1, FMT_SMR.1 Rationale: This SFR is related to the security attribute D.PSF_DATA, whose management must enforce ISD-R access control policy as well as ISD-P access control policy. For this reason the dependency is satisfied by the corresponding SFRs (FDP_ACC.1/ISDR and FDP_ACC.1/ISDP).
FMT_MSA.1/POL1	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FDP_IFC.1/SCP, FMT_SMF.1, FMT_SMR.1 Rationale: This SFR is related to the security attribute D.PROFILE_POL1, whose management must enforce Security Channel protocol information flow SFP, ISD-P access control SFP and ISD-R access control SFP. For this reason the dependency is satisfied by the corresponding SFRs (FDP_ACC.1/ISDR, FDP_ACC.1/ISDP and FDP_IFC.1/SCP).
FMT_MSA.1/CERT_KEYS	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FDP_IFC.1/SCP, FDP_ACC.1/ECASD, FMT_SMF.1, FMT_SMR.1 Rationale: This SFR is related to the security attributes <ul style="list-style-type: none"> • CERT.DP.ECDSA • CERT.SR.ECDSA • D.ISDP_KEYS • D.ISDR_KEYS • D.MNO_KEYS Their management must enforce Security Channel protocol information flow SFP, ISD-P access control SFP, ISD-R access control SFP and ECASD content access control SFP. For this reason the dependency is satisfied by the corresponding SFRs (FDP_ACC.1/ISDR, FDP_ACC.1/ISDP, FDP_ACC.1/ECASD and FDP_IFC.1/SCP).

FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_MSA.1/PSF_DATA, FMT_MSA.1/POL1, FMT_MSA.1/CERT_KEYS, FMT_SMR.1 Rationale: This SFR requires restrictive default values for the aforementioned security attributes. For this reason dependency is satisfied by all FMT_MSA.1 iterations.
FMT_SMF.1	No Dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1/EXT, FIA_UID.1/MNO-SD Rationale: this SFR is related to management functions, that require identification whether they are accessed by an external actor or by the MNO-SD. For this reason the dependency is satisfied by both FIA_UID.1/EXT and FIA_UID.1/MNOSD
FCS_COP.1/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.1/SCP, FCS_CKM.4/Mobile_network Rationale: The keys used by this SFR are distributed within the profiles during provisioning (FDP_ITC.1/SCP) and must be securely deleted (FCS_CKM.4/Mobile_network)
FCS_CKM.2/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2) and (FCS_CKM.4)	FDP_ITC.1/SCP, FCS_CKM.4/SCP-MNO Rationale: The keys in this SFR are the Mobile Network authentication keys included in the asset D.PROFILE_NAA_PARAMS. These keys are distributed as a part of the MNO profile during profile download (FDP_ITC.1/SCP) and must be securely deleted (FCS_CKM.4/Mobile_network)
FCS_CKM.4/Mobile_network	(FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2)	FDP_ITC.1/SCP Rationale: The keys in this SFR are the Mobile Network authentication keys included in the asset D.PROFILE_NAA_PARAMS. These keys are distributed as a part of the MNO profile during profile download (FDP_ITC.1/SCP)

Rationale for the exclusion of Dependencies:

The dependency FCS_CKM.2 or FCS_COP.1 of FCS_CKM.1/SCP-SM is discarded. The dependency to FCS_COP.1 is left unsatisfied, since the TOE uses the cryptographic libraries provided by its underlying Platform

The dependencies of FCS_COP.1/DRBG on FCS_CKM.1 or FDP_ITC.1 or FDP_ITC.2 and FCS_CKM.4 are re-assigned to FCS_RNG.1, as this is a Deterministic Random Bit Generator that, given a seed, provides cryptographic post-processing. The seed is provided by the PTG.2 random number generator. No specific key deletion is required, as it is overwritten as part of the normal operation.

9.1.2.5 SARs Dependency Rationale

This rationale shows that all dependencies of all security requirements have been addressed:

Requirement	Dependency	Satisfied by
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 12 SFR dependencies rationale

9.1.2.5.1 Rationale for the Security Assurance Requirements

EAL4 is required for this type of TOE and product since it is intended to defend against sophisticated attacks. This evaluation assurance level allows a developer to gain maximum assurance from positive security engineering based on good practices. EAL4 represents the highest practical level of assurance expected for a commercial grade product. In order to provide a meaningful level of assurance that the TOE and its embedding product provide an adequate level of defense against such attacks: the evaluators should have access to the low level design and source code. The lowest for which such access is required is EAL4.

9.1.2.5.2 ALC_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE and the embedding product. The standard ALC_DVS.1 requirement mandated by EAL4 is not enough. Due to the nature of the TOE and embedding product, it is necessary to justify the sufficiency of these procedures to protect their confidentiality and integrity. ALC_DVS.2 has no dependencies.

9.1.2.5.3 AVA_VAN.5 Advanced methodical vulnerability analysis

The TOE is intended to operate in hostile environments. AVA_VAN.5 "Advanced methodical vulnerability analysis" is considered as the expected level for Java Card technology-based products hosting sensitive applications. AVA_VAN.5 has dependencies on ADV_ARC.1, ADV_FSP.1, ADV_TDS.3, ADV_IMP.1, AGD_PRE.1 and AGD_OPE.1. All of them are satisfied by EAL4.

9.2 IC Composition rationale

9.2.1 Common Criteria rationale

Assurance level of the IC evaluation is EAL5 augmented by ALC_DVS.2 and AVA_VAN.5
Assurance level of the TOE is EAL4 augmented with ALC_DVS.2 and AVA_VAN.5.

Assurance level of the current evaluation is consistent with the assurance level in

9.2.2 Compatibility between threats (TOE and IC)

IC Threats	Rationale
BSI.T.Leak-Inherent	This threat is related to the information which is leaked from the TOE during usage of the Security IC in order to disclose sensitive data of the TOE. This threat has been considered in the current evaluation.
BSI.T.Phys-Probing	This threat is related to physical probing of the TOE to disclose relevant information. This threat has been considered in the current evaluation.
BSI.T.Malfunction	This threat is related to force malfunctions of the TSF due to environmental stress that could lower or bypass the implemented security mechanisms. This threat has been considered in the current evaluation.
BSI.T.PhysManipulation	This threat is related to physical manipulation of the Security IC. This is covered by the IC evaluation.
BSI.T.Leak-Forced	This threat is related to information which is leaked from the TOE during usage of the Security IC in order to disclose confidential user data of the composite TOE. This is covered by the IC evaluation.
BSI.T.Abuse-Func	This threat is related to the usage of functions of the TOE that are not allowed once the TOE Delivery and can impact the security of the TOE. This threat has been considered in the current evaluation.
BSI.T.RND	This threat is related to the deficiency of random numbers. This is covered by the IC evaluation.
AUG4.T.Mem-Access	The TOE implements memory access violation mechanisms based on the IC security policy. Therefore, this threat also covered by the TOE evaluation.
T.Confid-Applic-Code	Application code of the TOE is protected against unauthorized disclosure. Therefore, this threat also covered by the TOE evaluation.
T.Confid-Applic-Data	Application data of the TOE is protected against unauthorized disclosure. Therefore, this threat also covered by the TOE evaluation.
T.Integ-Applic-Code	Application code of the TOE is protected against unauthorized modification. Therefore, this threat also covered by the TOE evaluation.
T.Integ-Applic-Data	Application data of the TOE is protected against unauthorized modification. Therefore, this threat also covered by the TOE evaluation.

9.2.3 Compatibility between assumptions (TOE and IC)

IC Assumptions	Rationale
BSI.A.Process-Sec-IC	This assumption ensures the security of the delivery and storage of the IC. It is covered by the ALC_DVS.2 activity of the current TOE evaluation.

BSI.A.Resp-Appl	This assumption ensures that security relevant data of the current TOE are properly treated according to the IC security needs. It is covered by the ADV_IMP.1 activity of the TOE evaluation.
-----------------	--

9.2.4 Compatibility between security objectives for the environment (TOE and IC)

IC OEs	Rationale
BSI.OE.Resp-Appl	This objective deals with the treatment of TOE user data by the TOE itself. It is covered by the ADV_IMP.1 activity of the TOE evaluation.
BSI.OE.Process-Sec-IC	This objective is covered by the IC evaluation.
BSI.OE.Lim-Block-Loader	This objective is covered by the IC evaluation.

9.2.5 Compatibility between Security Objectives (TOE and IC)

BSI.O.Leak-Inherent	Also covered by the current evaluation.
BSI.O.Phys-Probing	Also covered by the current evaluation.
BSI.O.Malfunction	Also covered by the current evaluation.
BSI.O.Phys-Manipulation	Covered by the IC evaluation.
BSI.O.Leak-Forced	Covered by the IC evaluation.
BSI.O.Abuse-Func	Also covered by the current evaluation.
BSI.O.Identification	Covered by the IC evaluation.
BSI.O.RND	Covered by the IC evaluation.
BSI.O.Cap-Avail-Loader	Also covered by the ALC_DVS.2 activity of the current evaluation.
AUG1.O.Add-Functions	Covered by the IC evaluation.
AUG4.O.Mem-Access	Also covered by the current evaluation.
O.Controlled-ES-Loading	Also covered by the ALC_DVS.2 activity of the current evaluation.
O.Firewall	Also covered by the current evaluation.

9.2.6 Compatibility between Organisational Security Policies (TOE and IC)

IC Policies	Rationale
BSI.P.Process-TOE	This policy is related to the accurate unique identification during IC Development and Production. It was covered by the IC evaluation.
BSI.P.Lim-Block-Loader	Limiting and blocking the loader functionality for loading of Security IC Embedded Software. It was covered by the ALC_DVS.2 activity of the current TOE evaluation.
AUG1.P.Add-Functions	Additional Specific Security Functionality is provided by the IC, including NesLib. It was covered by the IC evaluation.
P.Controlled-ES-Loading	This policy is related to the capability provided by the TOE to load Security IC Embedded Software into the NVM after TOE delivery, in a controlled manner, during composite product manufacturing. It is covered by the ALC_DVS.2 activity of the current TOE evaluation.

P.Resp-AppI	It is related to the embedded software that is in the scope of the IC evaluation, and valid in case NesLib is embedded in the TOE. It was covered by the IC evaluation.
-------------	---

9.2.7 Compatibility between SFRs (TOE and IC)

IC SFRs are separated in the following groups as defined in [SOGIS-COMP]:

- IP_SFR: irrelevant IC SFR not being used by the current TOE.
- RP_SFR-SERV: relevant IC SFR being used by the current TOE to implement a security service with associated TSFI.
- RP_SFR-MECH: relevant IC SFR being used by the current evaluation because its security properties providing protection attacks to the TOE.

IC SFR	Rationale
FRU_FLT.2	RP_SFR-MECH
FPT_FLS.1	RP_SFR-MECH
FMT_LIM.1/Test	RP_SFR-MECH
FMT_LIM.2/Test	RP_SFR-MECH
FMT_LIM.1/Loader	RP_SFR-MECH
FMT_LIM.2/Loader	RP_SFR-MECH
FAU_SAS.1	RP_SFR-MECH
FDP_SDC.1	RP_SFR-MECH
FDP_SDI.2	RP_SFR-MECH
FPT_PHP.3	RP_SFR-MECH
FDP_ITT.1	RP_SFR-MECH
FPT_ITT.1	RP_SFR-MECH
FDP_IFC.1	RP_SFR-MECH
FCS_RNG.1	RP_SFR_SERV
FCS_COP.1/TDES	RP_SFR_SERV
FCS_COP.1/AES	RP_SFR_SERV
FCS_COP.1/RSA	RP_SFR_SERV
FCS_COP.1/ECC on Weierstrass curves	RP_SFR_SERV
FCS_COP.1/ECC on Edwards curves	IP_SFR
FCS_COP.1/SHA	RP_SFR_SERV
FCS_COP.1/Keccak and SHA-3	IP_SFR
FCS_COP.1/Keccak-p	IP_SFR
FCS_COP.1/Diffie-Hellman	IP_SFR
FCS_COP.1/DRBG	RP_SFR_SERV
FCS_CKM.1/Prime generation	RP_SFR_SERV
FCS_CKM.1/RSA key generation	IP_SFR
FDP_ACC.2/Memories	RP_SFR-MECH
FDP_ACF.1/Memories	RP_SFR-MECH

FMT_MSA.3/Memories	RP_SFR-MECH
FMT_MSA.1/Memories	RP_SFR-MECH
FMT_SMF.1/Memories	RP_SFR-MECH
FDP_ITC.1/Loader	RP_SFR-MECH
FDP_ACC.1/Loader	RP_SFR-MECH
FDP_ACF.1/Loader	RP_SFR-MECH
FMT_MSA.3/Loader	RP_SFR-MECH
FMT_MSA.1/Loader	RP_SFR-MECH
FMT_SMR.1/Loader	RP_SFR-MECH
FIA_UID.1/Loader	RP_SFR-MECH
FMT_SMF.1/Loader	RP_SFR-MECH
FDP_ACC.1/APPLI_FWL	RP_SFR-MECH
FDP_ACF.1/APPLI_FWL	RP_SFR-MECH
FMT_MSA.3/APPLI_FW	RP_SFR-MECH

10 Abbreviations and glossary

[CC]	Common Criteria
[EAL]	Evaluation Assurance Level
[LPU]	Library Protection Unit
[MPU]	Memory Protection Unit
[NVM]	Non-Volatile Memory
[ST]	Security Target
[TOE]	Target of Evaluation
[TSF]	TOE Security Functionality
[PP]	Protection Profile

11 References

- [ANSI X9.31] Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), ANSI X9.31-1998, American Bankers Association
- [AIS20/31] Bundesamt fuer Sicherheit in der Informationstechnik. AIS20/31: A proposal for: Functionality classes for random number generators, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.0, September 18th, 2011.
- [CERT-IC] ST33G1M2A and ST33G1M2M C01 Rapport de certification ANSI-CC-2020/23
- [CC31R5P1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction to General Model, Version 3.1, Revision 5, April 2016.
- [CC31R5P2] Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components, Version 3.1, Revision 5, April 2016.
- [CC31R5P3] Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components, Version 3.1, Revision 5, April 2016.
- [FIPS 46-3] FIPS PUB 46-3, Data Encryption Standard, October 25, 1999 (ANSI X3.92), National Institute of Standards and Technology
- [FIPS 81] FIPS PUB 81, DES Modes of Operation, April 17, 1995, National Institute of Standards and Technology
- [FIPS 140-2] FIPS PUB 140-2, Security requirements for cryptographic modules, March 2002 , National Institute of Standards and Technology
- [FIPS 180-2] FIPS PUB 180-2 Secure Hash Standard with Change Notice 1 dated February 25,2004, National Institute of Standards and Technology, U.S.A., 2004
- [FIPS 197] FIPS PUB 197, The Advanced Encryption Standard (AES) U.S. DoC/NIST, November 26, 2001
- [GP] Global Platform Inc., Global Platform Card Specification 2.3, October 2015. Document Reference: GPC_SPE_034
- [GP-SGBA] GlobalPlatform Card - Composition Model - Security Guidelines for Basic Applications - Version 1.0 - June 2012 – ref. GPC_GUI_050
- [GP-A] GlobalPlatform Inc., GlobalPlatform Technology, Confidential Card Content Management, Card Specification v2.3 – Amendment A, version 1.1.1, September 2018
- [GP-B] GlobalPlatform Inc., GlobalPlatform Card, Remote Application Management over HTTP, Card Specification v2.2 – Amendment B, Version 1.1.3, May 2015
- [GP-C] GlobalPlatform Inc., GlobalPlatform Technology, Contactless Services, Card Specification 2.3 – Amendment C, version 1.2.1, July 2018
- [GP-D] GlobalPlatform Inc., GlobalPlatform Card Technology, Secure Channel Protocol '03', Card Specification v2.2 – Amendment D, Version 1.1.1, July 2014

[GP-E]	GlobalPlatform Inc., GlobalPlatform Card Technology, Security Upgrade for Card Content Management Card Specification v2.3 – Amendment E, version 1.1, October 2016
[GP-SGBA]	GlobalPlatform Card - Composition Model - Security Guidelines for Basic Applications - Version 1.0 - June 2012 – ref. GPC_GUI_050
[GSMA SAS]	GSMA SAS Guidelines for Subscription Manager Roles GSMA SAS Methodology for Subscription Manager Roles GSMA SAS Standard for Subscription Manager Roles Version 2.0 - 13 May 2015
[IEEE 1363a]	IEEE Std 1363a-2004 Standard Specification of Public-Key Cryptography
[JCVM]	Java Card Virtual Machine Java Card Platform, Version 3.0.5, 2015, Oracle Technology Network
[JCAPI]	Java Card Application Programming Interfaces, Version 3.0.5, 2015, Oracle Technology Network
[JCRE]	Java Card Runtime Environment Specification, Classic Edition Version 3.0.5, 2015, Oracle Technology Network
[KS2011]	W. Killmann, W. Schindler, „A proposal for: Functionality classes for random number generators“, Version 2.0, September 18, 2011
[MILENAGE]	3GPP TS 35.205, 3GPP TS 35.206, 3GPP TS 35.207, 3GPP TS 35.208, 3GPP TR 35.909 (Release 11): "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*"; <ul style="list-style-type: none"> • Document 1: General • Document 2: Algorithm Specification • Document 3: Implementers Test Data • Document 4: Design Conformance Test Data • Document 5: Summary and results of design and evaluation
[PP-eUICC]	Embedded UICC Protection Profile, Version 1.1, 25/08/2015
[PP-IC]	Security IC Platform Protection Profile with Augmentation Packages Version 1.0 - BSI-CC-PP-0084-2014
[PP-JC]	Java Card System - Open Configuration Protection Profile, December 2017, Version 3.0.5
[SGP.02]	GSMA, SGP.02 Remote Provisioning Architecture for Embedded UICC Technical Specification, v4.2 July 2020
[SOGIS-COMP]	Composite product evaluation for Smart Cards and similar devices, version 1.5.1, May 2018
[ST-IC]	ST33G1M2A and ST33G1M2M C01 Security Target for composition version C01.4, Mar 2021. Reference SMD_ST33G1M2AM_ST_19_002 Rev C01.4.

- [TS 33 102] 3GPP TS 33.102 “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 12)”
- [TS 102 221] ETSI, TS 102 221, UICC-Terminal interface; Physical and logical characteristics, Version 15.2.0, May 2019
- [TS 102 222] ETSI, TS 102 222, Administrative commands for telecommunications applications, Version 15.0.0, June 2018
- [TS 102 223] ETSI, TS 102 223, Card Application Toolkit (CAT), Version 15.2.0, June 2019
- [TS 102 224] ETSI, TS 102 224, Security mechanisms for UICC based Applications, Functional requirements, Version 14.0.0, September 2018
- [TS 102 225] ETSI, TS 102 225, Secured packet structure for UICC based applications, Version 13.0.0, July 2018
- [TS 102 226] ETSI, TS 102 226, Remote APDU structure for UICC based application, Version 10.0.0, March 2013
- [NISTSP800-90] NIST SP 800-90 NIST Special Publication 800-90, Recommendation for random number generation using deterministic random bit generators (Revised), National Institute of Standards and Technology (NIST), March 2007
- [TUAK] 3GPP TS 35.231, 3GPP TS 35.232, 3GPP TS 35.233 (Release 12)
- Document 1: Algorithm specification
 - Document 2: Implementers’ test data
 - Document 3: Design conformance test data