NXP JCOP 5.2 on SN100.C58 Secure Element

Security Target Lite

Rev. 3.2 — 17 June 2021
NSCIB-CC-0023577

Product evaluation document
CC PUBLIC

Document information

Information	Content
Keywords	Common Criteria, Security Target, NXP JCOP 5.2 on SN100.C58 Secure Element
Abstract	This document contains information to fulfill the requirements of the Common Criteria component ASE (Security Target) for the Evaluation of the NXP JCOP 5.2 on SN100.C58 Secure Element developed and provided by NXP Semiconductors, Business Unit Security and Connectivity, according to the Common Criteria for Information Technology Security Evaluation Version 3.1 at EAL5 augmented.

Revision History

Rev.	Date	Description
1.0	2019-11-26	First release.
2.0	2020-06-12	Add JCOP 5.2 R2 to the certification scope, use uniform JCOP naming
2.1	2020-09-30	Fix PID format description and re-title Table12 as an example, for consistency.
3.0	2021-05-03	Add R3 to scope
3.1	2021-06-14	Update table 2 Micro-controller cert to NSCIB-21-174263
3.2	2021-06-17	Update SN100 ST reference - Add SMIC manufacturing site, H/W cert NSCIB-21-174263/2

1 ST Introduction (ASE_INT)

1.1 ST Reference and TOE Reference

Table 1. ST Reference and TOE Reference

ST Title	NXP JCOP 5.2 on SN100.C58 Secure Element Security Target Lite
ST version	Revision 3.2
TOE name	NXP JCOP 5.2 on SN100.C58 Secure Element
TOE version	R1 - R1.01.1 R2 - R2.01.1, R2.02.1 and R2.03.1
Product Type	Secure Element and Software Stack
CC Version	Common Criteria for Information Technology Security Evaluation Version 3.1, Revision 5, April 2017 (Part 1 [1], Part 2 [2] and Part 3 [3])

1.2 TOE Overview

1.2.1 TOE components

The overall product consists of a Secure Micro-Controller and a software stack.

The **Micro-Controller** provides an Integrated NFC controller and an embedded Secure Element core.

The **software stack** creates 2 separate domains to provide a converged product consisting of a familiar Java Card Secure Element domain and an eUICC domain providing UICC functionality in accordance with the GSMA Specification [40] and external ISO-7816 connectivity. The eUICC domain at the platform level is underpinned by the same Java Card and Global Platform technology as the eSE domain, but is dedicated to the eUICC application.

The TOE domains and communication interfaces are depicted in Figure 1 and the constituent components are described in more detail in Section 1.3.

Note: care should be taken to discern the concept of eSE and eUICC domains which are notional concepts to distinguish the eUICC application, accessible by ISO-7816 communications channels, from the familiar Java Card Open platform, accessible via the system mailbox and NFC controller or SPI Interfaces. The use of the term domain in this context is distinct from the definition of domain as per GlobalPlatform [26], which are instantiated and found within the notional domains, such as the ISD in the eSE Domain.

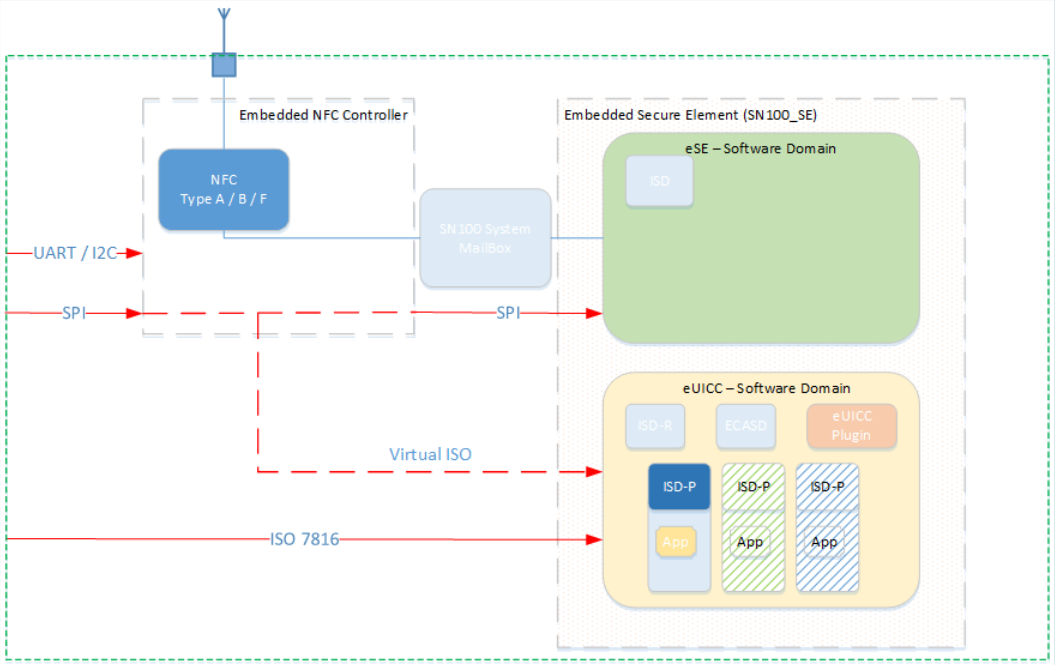

Figure 1. JCOP 5.2 Domains and Communication Interfaces

Both of the Domains, eSE and eUICC, are running on the eSE core of the micro-controller.

The interface to the eSE domain is provided by the System Mailbox, which is connected to the embedded NFC Controller. All eSE communications must support HCI protocol. The integrated NFC controller provides up to 4 gates for external users to communicate with the TOE supporting Card Emulation Mode Type A, Type B and Type F as well as a wired Interface using APDUCard Gate. The TOE also supports SPI communication directly with the eSE domain and ISO 7816 communication directly with an eUICC domain.

The software stack can be further split several components represented on the figure below and detailed in following.

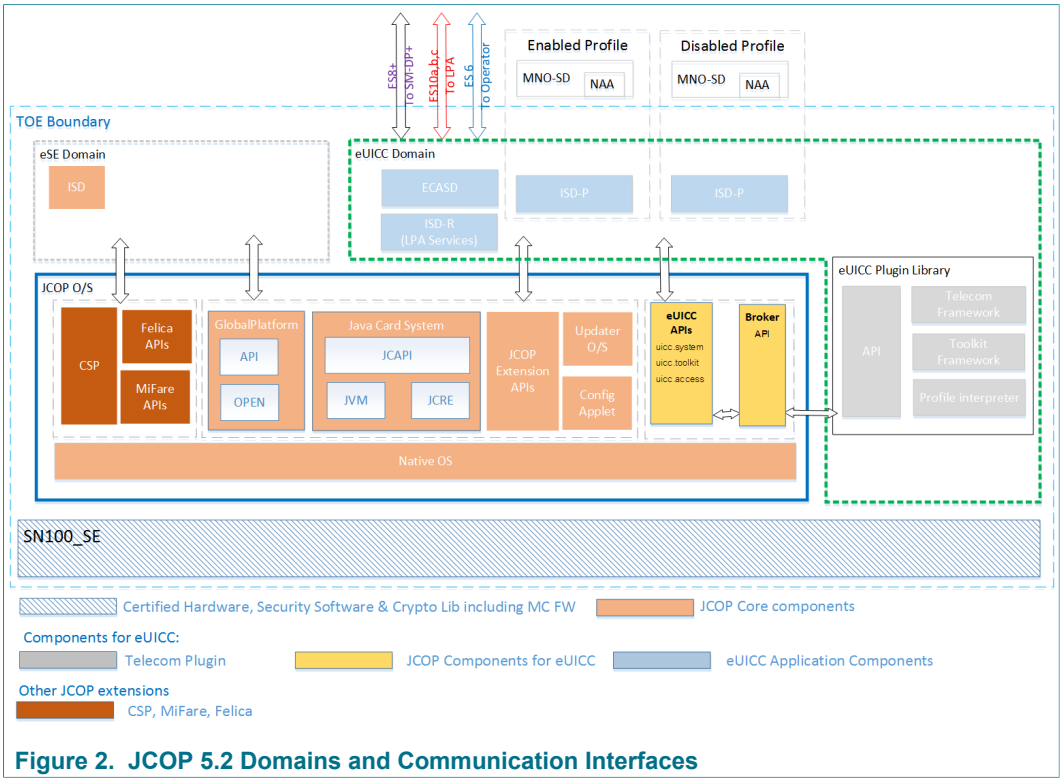

Figure 2. JCOP 5.2 Domains and Communication Interfaces

This figure shows the components of the JCOP O/S including the extension APIs for MiFare, Felica, eUICC and CSP. It also shows the Config Applet which has special privileges and is used to personalise and configure the TOE. The eUICC APIs provide access to NXP proprietary functions and a broker API which forwards eSIM/SIM/UICC/ISIM commands to an eUICC plugin library.

1.2.1.1 JCOP component

The base of the product is composed of:

- Firmware for booting and low level functionality of the Secure Element, called MC FW - included in the hardware certification.
- Software for implementing cryptographic operations on the Secure Element, called Security Software - included in the hardware certification.
- Software to update JCOP5.2 OS or UpdaterOS, called OS Update Component.
- Software for implementing JCOP5.2 OS:
  - Software that implements low level functionality, called Native OS.
  - Software that implements the Java Card Virtual Machine [24], called JCVM
  - Software that implements the Java Card Runtime Environment [25], called JCRE
  - Software that implements the Java Card Application Programming Interface [23], called JCAPI.
  - Software for implementing content management according to GlobalPlatform [26], called GP.
  - Software that implements a proprietary programming interface, called Extension API.
  - Software that handles personalization and configuration, called Config Applet.
  - Software that implements the API and functionality for MiFare - no security claims are made on MiFare.

- Software that implements the API and functionality for Felica - no security claims are made on Felica.
- Software that implements NXP Proprietary API for eUICC implementations, called eUICC API.
- Other APIs (e.g. OSCCA, UAI) for wich no security claims are made.

1.2.1.2 eUICC component

The eUICC component implements the GSMA RSP architecture following [38] and [39] specifications. (Note: For R3 version all references to [38] should be considered as [39].

It is composed of:

- The Application Layer: privileged applications, such as Security Domains, providing the remote provisioning and administration functionality - the notion of Security Domain follows the definition given by [35]
  - An ISD-R, including LPA Services, providing life-cycle management of profiles;
  - ECASD providing secure storage of credentials and security functions for key establishment and eUICC authentication;
  - ISD-P security domains, each one hosting a unique profile.
- The Platform Layer: a set of functions providing support to the Application Layer:
  - A Telecom Framework providing network authentication algorithms;
  - A Profile Package Interpreter translating Profile Package data into an installed Profile;
  - And a Profile Policy Enabler which comprises Profile Policy verification and enforcement functions.
- The software that allows forwarding of SIM/UICC/USIM/ISIM API calls to 3rd party Plugin, called Broker API.

1.2.1.3 CSP component

The CSP JavaCard extension implements a Cryptographic Service Provider (CSP) following [43] specifications.

1.2.1.4 TOE packages

The TOE provides Java Packages with Global Scope or restricted to one or other of the available Domains (eSE or eUICC).

1.2.1.4.1 Global packages

- Packages with Global Scope
  - java.lang.cap
  - java.io.cap
  - javacard.framework.cap
  - javacard.security.cap
  - org.globalplatform.cap
  - org.globalplatform.contactless.cap
  - org.globalplatform.upgrade.cap
  - javacardx.crypto.cap
  - javacardx.apdu.cap
  - javacardx.apdu.cap
  - javacardx.external.cap
  - uicc.hci.framework.cap

- uicc.hci.services.cardemulation.cap
- uicc.hci.services.connectivity.cap
- uicc.hci.services.readermode.cap
- com.nxp.id.jcop.os.cap
- com.nxp.id.jcop.javacard.security.cap
- com.nxp.id.jcop.hci.cap
- com.nxp.id.jcop.oscca.cap
- com.nxp.id.jcopx.security.cap
- com.nxp.id.jcopx.util.cap
- com.nxp.id.jcopx.authority.cap
- com.nxp.id.jcopx.migration.cap
- com.nxp.id.jcop.globalplatform.cap
- com.nxp.id.jcop.globalplatform.auxiliary.cap
- com.nxp.id.jcop.globalplatform.auxiliary2.cap
- com.nxp.id.jcop.globalplatform.auxiliary3.cap
- com.nxp.id.jcop.uicc.globalplatform.security.cap
- com.nxp.id.jcopx.tearing.cap
- com.nxp.id.jcopx.accelerator.cap
- com.nxp.id.jcopx.globalplatform.contact.cap
- com.nxp.id.jcopx.systemstack.cap
- com.nxp.id.jcopx.osupdate.cap
- com.nxp.id.jcop.uiccframework.cap
- com.nxp.id.jcopx.oscca.cap
- com.nxp.id.jcopx.v2xsupport.cap
- javacardx.framework.util.intx.cap

1.2.1.4.2 JCOP packages

- Packages with scope restricted to the eSE Domain
  - org.mifare4mobile.hostinterface.cap
  - org.mifare4mobile.walletInterface.cap
  - org.mifare4mobile.parser.cap
  - org.mifare4mobile.userverifier.cap
  - com.nxp.id.jcop.mifare4mobile.cap
  - com.nxp.id.jcopx.commerce.cap
  - com.nxp.id.jcop.config_applet_v2.cap
  - com.nxp.id.jcop.configapplet.cap
  - com.nxp.id.jcopx.mifare.mifaredesfire.cap
  - com.nxp.id.jcopx.m4mext.cap
  - com.nxp.id.jcopx.mifare.mifareplus.cap
  - com.nxp.id.jcopx.mifare.mifarecommon.cap
  - com.sony.javacard.crypto.cap
  - com.sony.javacard.crypto.advance.cap
  - com.sony.javacard.crypto.a4.cap
  - com.sony.javacard.crypto.a5.cap
  - com.sony.javacard.crypto.a6.cap
  - com.sony.javacard.crypto.advance.e3.cap
  - com.sony.javacard.crypto.advance.e4.cap

– com.sec.mobile.fra.cap
– com.nxp.id.jcopx.ioaccess.cap

1.2.1.4.3 eUICC packages

- Packages with scope restricted to the eUICC Domain
  – com.nxp.id.jcop.euicc.cap
  – com.nxp.id.jcop.euicc.gsmalib.cap
  – com.nxp.id.jcopx.euicc.gsma.cap
  – com.nxp.id.jcopx.uicc.globalplatform.cap
  – com.nxp.id.jcopx.blob.cap
  – com.nxp.id.jcopx.uicc.auth.cap
  – com.nxp.id.jcopx.uicc.system.cap
  – com.nxp.id.jcopx.uicc.toolkit.cap
  – com.nxp.id.jcopx.uicc.interfacebroker.cap
  – com.nxp.id.jcopx.uicc.interfacebroker.sim.cap
  – com.nxp.id.jcopx.uicc.interfacebroker.uicc.cap
  – uicc.access.cap
  – uicc.access.fileadministration.cap
  – uicc.isim.access.cap
  – uicc.services.highupdatearray.cap
  – uicc.system.cap
  – uicc.toolkit.cap
  – uicc.usim.access.cap
  – uicc.usim.geolocation.cap
  – uicc.usim.toolkit.cap
  – sim.access.cap
  – sim.toolkit.cap
- eUICC specific packages added in R2
  – uicc.usim.suci.cap

1.2.1.4.4 CSP packages

- Packages with scope restricted to CSP
  – de.bsi.csp

1.2.2 TOE usage and major features

The usage of the TOE is focused on security critical applications in small form factors. One main usage scenario is the use in mobile phones, which can use the TOE to enable mobile payment or mobile ticketing with the phone based on the security of the TOE.

The TOE provides a variety of security features. The hardware of the Micro Controller already protects against physical attacks by applying various sensors to detect manipulations and by processing data in ways which protect against leakage of data by side channel analysis. With the software stack the TOE provides many cryptographic primitives for encryption, decryption, signature generation, signature verification, key generation, secure management of PINs and secure storage of confidential data (e.g. keys, PINs). Also the software stack implements several countermeasures to protect the TOE against attacks.

The TOE includes the following features:

- Cryptographic algorithms and functionality:
  - 3DES for en-/decryption (CBC and ECB) and MAC generation and verification (2-key 3DES, 3-key 3DES, Retail-MAC, CMAC and CBC-MAC).
  - AES (Advanced Encryption Standard) for en-/decryption (GCM, CBC and ECB) and MAC generation and verification (CMAC, CBC-MAC).
  - RSA and RSA CRT for en-/decryption and signature generation and verification.
  - RSA and RSA CRT key generation.
  - SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 hash algorithm.
  - Secure SHA-1, Secure SHA-224, Secure SHA-256, Secure SHA-384, Secure SHA-512 hash algorithm.
  - HMAC
  - ECC over GF(p) for signature generation and verification (ECDSA).
  - ECC over GF(p) key generation for key agreement.
  - Random number generation according to class DRG.3 of AIS 20 [46]
- Java Card 3.0.5 functionality:
  - Executing Java Card bytecodes.
  - Managing memory allocation of code and data of applets.
  - Enforcing access rules between applets and the JCRE.
  - Mapping of Java method calls to native implementations of e.g. cryptographic operation.
  - Garbage Collection fully implemented with complete memory reclamation including compactification.
  - Support for Extended Length APDUs.
  - Persistent Memory Management and Transaction Mechanism.
- GlobalPlatform 2.3 functionality including Amendments A,B,C,D,E,F,H and I and is compliant with the Common Implementation Configuration.
  - Loading of Java Card packages.
  - Instantiating applet instances.
  - Java package deletion.
  - Java applet instance deletion.
  - Creating Supplementary Security Domains.
  - Associating applets to Security Domains.
  - Installation of keys.
  - Verification of signatures of signed applets.
  - CVM Management (Global PIN) fully implemented.
  - Secure Channel Protocol is supported.
  - Delegated Management, DAP (RSA 1024 and ECC 256).
  - Compliance to Secure Element configuration.
- GSMA 'Remote SIM Provisioning Architecture for consumer Devices', version 2.2.1 [38] and v2.2.2 [39]
- Cryptgraphic Service Provider features, [43]
- NXP Proprietary Functionality:
  - Felica functionality accessible via Applets using the Felica API - no security functionality is claimed for this functionality.
  - Config Applet: JCOP5.2 OS includes a Config Applet that can be used for configuration of the TOE.

– OS Update Component: Proprietary functionality that can update JCOP5.2 OS or UpdaterOS.
– Restricted Mode: In Restricted Mode only very limited functionality of the TOE is available such as, e.g.: reading logging information or resetting the Attack Counter.
– Error Detection Code (EDC) API.

Functionality introduced in R2, for which there are no specific additional security claims

- CAT-TP, with limitations as described in the UGM [13], Section 8.1(20)
- 5G features as per SIM Alliance 2.3, see [13] Section 2.4.4. and 8.1(15)
- Extension to Global Platform Amendment H, UGM see [13] Section 3.5.7
- CPLC data made available through SystemInfo, UGM see [13] Section 2.1.3.22

Changes in R3, for which there are no specific additional security claims

- R3 is compliant to the GSMA SGP.22 version 2.2.2 June 2020 [39], whilst previous versions are (R1 and R2) are compliant to GSMA SGP.22 version 2.2.1 Dec 2018 [38]
- CAT-TP is not supported in R3 product
- UAI query extended to include Amendment H Status [19] Section 7.1.2
- Addition of 5th Logical Channel [19] Section8.4

1.2.3 TOE Type

The TOE type is software and certified hardware platform (including hardware, firmware and crypto library).

The platform part is a Java Card with GP functionality. It can be used to load, install, instantiate and execute off-card verified Java Card applets. The eSE domain, which is externally accessible via SPI or by the System mailbox which is connected to an Integrated NFC controller, supporting Type A,B and F contactless communications. The NFC controller and system mailbox are not within the scope of the evaluation. This TOE includes a dedicated eUICC Domain which is directly accessible by the ISO-7816 interface.

The eUICC part is a UICC embedded in a consumer device and may be in a removable form factor or otherwise. It connects to a given mobile network, by means of its currently enabled MNO profile.

1.2.4 Non-TOE Hardware/Software/Firmware

Three groups of users shall be distinguished here.

- The first group is the **end-users** group, which uses the TOE with one or more loaded applets in the final form factor as an embedded Secure Element. These users only require a communication device to be able to communicate with the TOE. The eSE domain of the TOE communicates via the Secure Mail Box, which is connected to the Integrated NFC controller and also supports an SPI interface with the NFC controller. The NFC controller facilitates contactless or wired interfaces supporting:
  – Card Emulation Type A, Type B and Type F according to ETSI 102 622 [44].
  – Wired Mode by using the APDUCard Gate according to ETSI 102 622 [44].
  The wired interface is expected to be connected to an applications processor.
  The eUICC domain of the TOE communicates directly via the ISO-7816 interface or via a Virtual ISO over SPI.

- The second group of users are **administrators of cards**. They can configure the TOE by using the Config Applet or install additional applets. These users require the same equipment as end-users.
- The third group of users develops Java Card applets and executes them on the TOE. These **applet developers** need in addition to the communication device a set of tools for the development of applets. This set of tools can be obtained from the TOE vendor and comprises elements such as PC development environment, byte code verifier, compiler, linker and debugger.

1.3 TOE Description

1.3.1 TOE scope

The current TOE scope covers the following components:

- The certified certified NXP SN100 Secure Element and Crypto LibrarySecure.
- The JavaCard platform in open configuration.
- The eUICC implementation in composition with the certified certified NXP SN100 Secure Element and Crypto LibrarySecure
- The CSP JavaCard extension.

Note that the NFC controller and the system mailbox are not in the scope of the evaluation.

The TOE can be in two configurations: with access to eUICC component or not, depending whether the ISO7816 is enabled; in any case, both configuration are in the scope of the evaluation.

The TOE is uniquely deployed on the C58 variant of the SN100 Secure Element, therefore all reference to the SN100 Secure element in this document implies the C58 variant. This may also be referred to as SN100.C58.

The CSP extended package is active in all configurations.

1.3.2 TOE components details

The certification of this TOE is a composite certification. This means that for the certification of this TOE other certifications of components which are part of this TOE are re-used. In the following sections more detailed descriptions of the components of Figure 1 are provided. In the description it is also made clear whether a component is covered by a previous certification or whether it is covered in the certification of this TOE.

1.3.2.1 Micro Controller component details

The Micro Controller is a secure element from NXP based on ARM architecture. The Micro Controller contains a co-processor for symmetric cipher, supporting AES and DES operations, and a co-processor for asymmetric algorithms. It contains volatile (RAM) memory and non-volatile Flash memory. The product design is based on smart card technology and is interchangeably referred to as a secure element or smart card product. The Micro Controller has been certified in a previous certification and the results are re-used for this certification. The exact reference to the previous certification is given in the following Table 2:

Table 2. Reference to Certified Micro Controller

Hardware Commercial Name	NXP SN100 Series Secure Element with Crypto Library
Certified HW Version	SN100_SE B2.1 C58
Certification ID	NSCIB-21-174263/2
Shortened Identifier	SN100.C58
Security Target Reference	[22]

1.3.2.1.1 MC FW (Micro Controller Firmware)

The Micro Controller Firmware is used for testing of the Micro Controller at production, for booting of the Micro Controller after power-up or after reset, for configuration of communication devices.

The MC FW has been certified in a previous certification. It has been certified together with the Micro Controller and the same references ([22]) as given for the Micro Controller also apply for the MC FW.

1.3.2.1.2 Security Software

The Security Software is used by the IC Embedded Software and provides cryptographic functionality (CryptoLib) but also an interface for memory erasing and programming (Flash Services). The Crypto Lib is included in the hardware certification [22].

1.3.2.2 JCOP component details

1.3.2.2.1 JCOP5.2 OS

JCOP5.2 OS consists of Native OS, JCVM, JCRE, GP framework, JCAPI, Extension API and Config Applet. JCVM, JCRE, JCAPI and GP framework are implemented according to the Java Card Specification and GlobalPlatform version listed below.

Table 3. Java Card Specification Versions

JCRE	Version 3.0.5 Classic Edition [25]
JCVM	Version 3.0.5 Classic Edition [24]
JCAPI	Version 3.0.5 Classic Edition [23]

Table 4. Global Platform Specifications and Amendments

Name	Version	Security Claimed	eSE domain
GP Framework	Version 2.3 [26]	yes	yes
Amendment A, Confidential Card Content Management	Version 1.1 [28]	yes	yes
Amendment B, Remote Application Management over HTTP	Version 1.1.3 [29]	yes	no
Amendment C, Contactless Services	Version 1.1 [31]	yes	yes
Amendment D, Secure Channel Protocol '03'	Version 1.1.1 [32]	yes	yes

Name	Version	Security Claimed	eSE domain
Amendment E, Security Upgrade for CCM	Version 1.0.1 [33]	yes	yes
Amendment F, Secure Channel Protocol '11'	Version 1.1 [34]	yes	yes
Amendment H, Executable Load File Upgrade	Version 1.1 [35]	no	yes
Amendment I, Secure Element Management Service (SEMS)	Version 1.0 [36]	no	yes
Common Implementation Configuration	Version 2.0 [37]	no	yes
UICC Configuration	Version 1.0.1 [41]	no	yes
UICC Configuration - Contactless Extension	Version 1.0 [42]	no	yes

JCOP5.2 OS components version can be identified by using the GET PLATFORM IDENTIFIER command. This command returns the card identification data, which includes the Hardware Type, JCOP Version, Build Number, Mask ID, a Patch ID and Non-Volatile Memory Size. The Platform ID is a data string that allows to identify the JCOP5.2 OS component

1.3.2.2.2 Native Applications

The Native Applications extend the available cryptographic algorithms for the Security Software. These Native Applications are proprietary implementations (e.g. Felica) which make use of the Security Software's security mechanisms. Native Applications are provided to JCOP5.2 OS via the Security Software. No security functionality claimed for Native Applications, it is an extension to the Crypto Lib.

1.3.2.2.3 OS Update Component

The OS Update Component can update JCOP5.2 OS and UpdaterOS and contains two main components:

- OsSelector (no security claimed): After a hardware reset it provides the functionality to either boot UpdaterOS or JCOP5.2 OS. OsSelector also ensures that
  - only one OS is active (running) at a time.
  - at any time, at least one OS can be booted.
  - an invalid OS (e.g. partly flashed) can never be booted.
- UpdaterOS:
  - it handles APDUs to write a new OS (either JCOP5.2 OS or UpdaterOS) to flash.
  - it verifies the integrity of the new OS before updating.
  - it decrypts the new OS before updating.
  - it checks if the new OS can be authenticated and checks if the update can be authorized.
  - it ensures that the activation and setting of the information that identifies the new OS is done atomically.
  - if the update fails the system stays in a secure state.

The UpdaterOS is a standalone operating system that can only be active when JCOP5.2 OS is not active. Besides the capability to update JCOP5.2 OS, UpdaterOS is also

capable to update itself. The UpdaterOS version can be queried by using a SELECT OS Update AID Command (see UGM [10] or [13]). UpdaterOS shares parts of the Native OS with JCOP5.2 OS, e.g.: communication interface, wrapper to Security Software (Flash Services and CryptoLib).

1.3.2.3 eUICC component details

The eUICC 3rd party plugin provides interpretation of the Telecom commands defined in ETSI TS 102 222, ETSI TS 102 221, ETSI TS 131 102, ETSI TS 131 103, 3GPP2 C.S00065-0, and all the support of CAT API (defined in ETSI TS 143 019, ETSI TS 102 241, ETSI TS 131 130). This plugin uses the security and cryptographic services provided by the JCOP platform. The plugin is only available on the eUICC domain and is identifiable through Global Platform GET EUICC PLUGIN VERSION command as explained in Section 1.4

1.3.2.4 CSP component details

The CSP component is a JavaCard package extension exposing a Java Card CSP API to other JavaCard applications.

It implements a platform architecture defined in the CSP PP i.e. users are other applications running on top of the JCOP platform. The JCOP platform provides the required secure execution environment while the CSP JavaCard package provides the secure services implementation.

Table 5. CSP Application Identification

Registered AID	E804007F00070308
Version	0.2

1.3.3 TOE Life Cycle

1.3.3.1 TOE Life Cycle

The life cycle for this TOE is based on the general smart card life cycle defined in the Java Card Protection Profile - Open Configuration [6], but also considers the life-cycle presented by the GSMA Embedded UICC for Consumer Devices Protection Profile [7], both of which are mapped to the lifecycle presented in BSI-PP-0084 [5], see Figure 3. The JCOP lifecycle is fully described in table1.8, whilst the eUICC application lifecycle is covered in table 1.9 in Section 1.4.2.1.

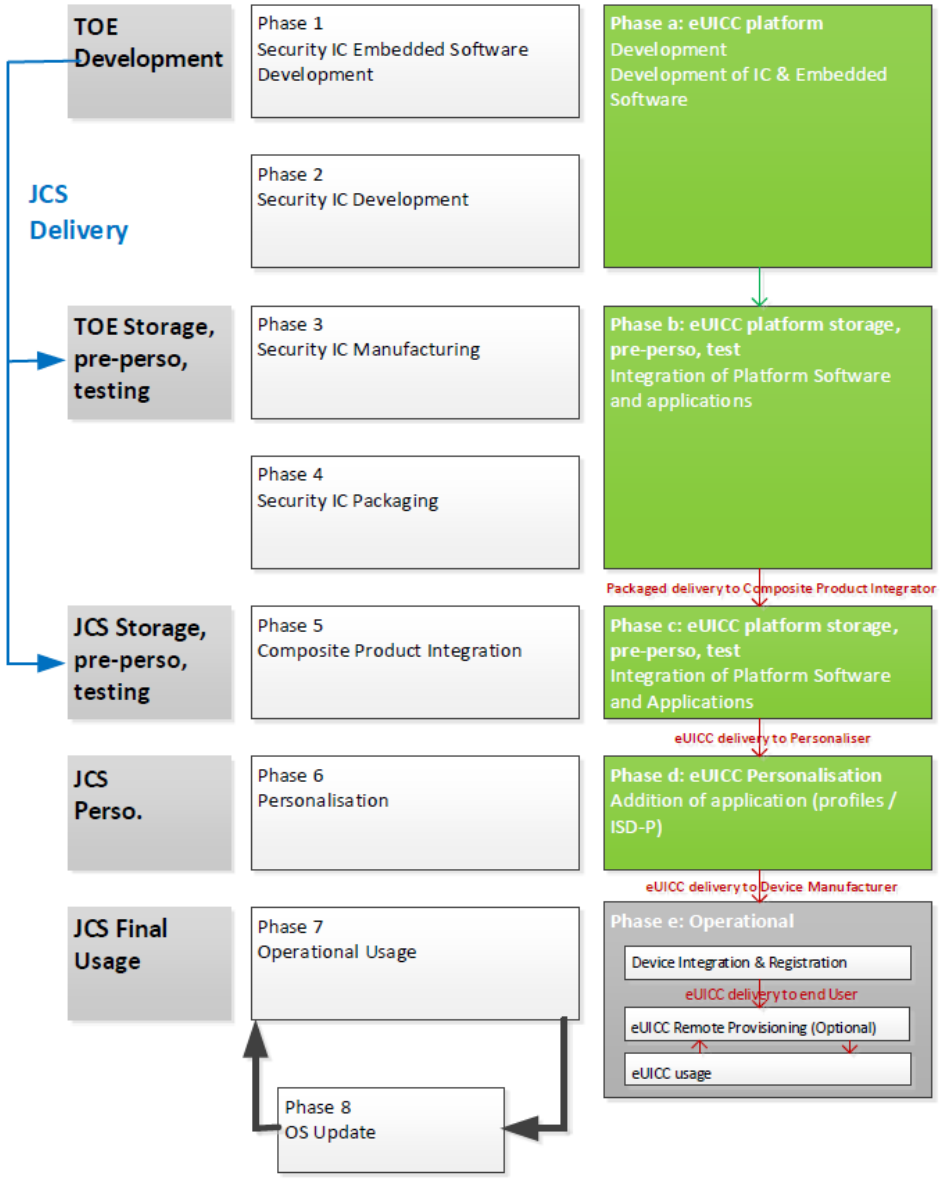

Figure 3. TOE Life Cycle within Product Life Cycle

Table 6. Life-cycle

Phase	Name	Description
1	Security IC Embedded Software Development	The IC Embedded Software Developer is in charge of • smartcard embedded software development including the development of Java Card applets and • specification of IC pre-personalization requirements, though the actual data for IC pre-personalization comes from phase 4, 5, or 6.
2	Security IC Development	The IC Developer • designs the IC, • develops IC Dedicated Software, • provides information, software or tools to the IC Embedded Software Developer, and • receives the embedded software from the developer, through trusted delivery and verification procedures. From the IC design, IC Dedicated Software and Smartcard Embedded Software, the IC Developer • constructs the smartcard IC database, necessary for the IC photomask fabrication.
3	Security IC Manufacturing	The IC Manufacturer is responsible for • producing the IC through three main steps: IC manufacturing, IC testing, and IC pre-personalization. The IC Mask Manufacturer • generates the masks for the IC manufacturing based upon an output from the smarcard IC database. Configuration items may be changed/deleted.
4	Security IC Packaging	The IC Packaging Manufacturer is responsible for • IC packaging and testing.
5	Composite Product Integration	The Composite Product Manufacturer is responsible for the smartcard product finishing process.
6	Personalization	The Personalizer is responsible for • smartcard (including applet) personalization and final tests. User Applets may be loaded onto the chip at the personalization process and configuration items may be changed/deleted. The Config Applet can be used to set Configuration Items.

Phase	Name	Description
7	Operational Usage	The Personalizer is responsible for • smartcard product delivery to the smartcard end-user, and the end of life process. • applets may be loaded onto the chip. • triggering an OS update. • Config Applet: changing Config Items. • perform card content management according to Global Platform and Amendments specifications.

The evaluation process is limited to phases 1 to 5. User Applet development is outside the scope of this evaluation. Applets can be loaded into Flash memory. Applet loading into Flash memory can be done in phases 3, 4, 5, and 6. Applet loading in phase 7 is also allowed. This means post-issuance loading of applets can be done for a certified TOE. The certification is only valid for platforms that return the Platform Identifier as stated in Table 8. The delivery process from NXP to their customers (to phase 4 or phase 5 of the life cycle) guarantees, that the customer is aware of the exact versions of the different parts of the TOE as outlined above. TOE documentation is delivered in electronic form (encrypted according to defined mailing procedures).

Note: Phases 1 to 3 are under the TOE developer scope of control. Therefore, the objectives for the environment related to phase 1 to 3 are covered by Assurance measures, which are materialized by documents, process and procedures evaluated through the TOE evaluation process. During phases 4 to 7 the TOE is no more under the Evaluation Version developer control. In this environment, the TOE protects itself with its own Security functions. But some additional usage recommendation must also be followed in order to ensure that the TOE is correctly and securely handled, and that shall be not damaged or comprised. This ST assumes (A.USE_DIAG, A.USE_KEYS) that users handle securely the TOE and related Objectives for the environment are defined (OE.USE_DIAG, OE.USE_KEYS).

1.3.3.2 eUICC specific life-cycle

The eUICC life-cycle is composed of the following stages as described by GSMA - Embedded UICC for Consumer Devices Protection Profile [7]:

Table 7. eUICC lifecycle stages and Delivery Options

Phase	Description
a	Development corresponds to the first two stages of the IC development;
b	Storage, pre-personalisation and test cover the stages related to manufacturing and packaging of the IC; • TOE Delivery [optional]: At this phase the delivery of the TOE to the customer of the eUICC manufacturer could happen, if the TOE is already self-protected;
c	eUICC platform storage, pre-personalization, test covers the stage of the embedding of software products onto the eUICC; • TOE Delivery [optional]: At this phase the delivery of the TOE to the customer of the eUICC manufacturer could happen, if the TOE is already self-protected;
d	eUICC personalization covers the insertion of provisioning Profiles and Operational Profiles onto the eUICC; • TOE Delivery [optional]: At this phase the delivery of the TOE to the customer of the eUICC manufacturer happens at the latest;

Phase	Description
e	operational usage of the TOE covers the following steps: • eUICC integration onto the Device is performed by the Device Manufacturer. The Device Manufacturer and/or the eUICC Manufacturer also register the eUICC in a given SM-DS; • The eUICC is then used to provide connectivity to the Device end-user. The eUICC may be provisioned again, at post-issuance, using the remote provisioning infrastructure.

The eUICC product will be delivered at the end of Phase c.

1.3.3.3 CSP specific life-cycle

The CSP life-cycle follows the JCOP life cycle in compliance with the CSP PP [8]

1.3.4 TOE delivery information

1.3.4.1 Delivery method

The TOE is shipped to the customer by NXP as embedded firmware on the certified Hardware Platform. The available documentation can be downloaded by customers in PDF format directly from the NXP DocStore.

1.3.4.2 Delivery form factor

The only commercially available package type is "Wafer Level Chip Scale Package" (WLCSP). This package is a thin fine-pitch ball grid array package. All (enabled) pins of the TOE are externally accessible. Any additional security provided by the package is ignored for the security of the TOE and therefore the package type is not security relevant.

1.3.4.3 Delivery content

The delivery comprises the TOE and an associated set of UGM documentation (note: each TOE revision has it's own specific set of UGM documents and it follows naturally that where mention is made of reference to the UGM or addendum, the user should ensure that they are referencing the correctly associated document):

Table 8. JCOP5.2 R1.01.1 Delivery Items

Type	Name	Version
Product	NXP JCOP 5.2 on SN100.C58 Secure Element including software (JCOP5.2 OS, native applications and OS Update Component) that is identified by Platform ID.	see Table 12
Document	JCOP 5.2 R1.01.1 User Guidance Manual	see [10] (pdf)
Document	JCOP 5.2 R1.01.1 User Guidance Manual Addendum for SEMS API	see [11] (pdf)
Document	JCOP 5.2 R1.01.1 User Guidance Manual Addendum for CSP API	see [12] (pdf)

Table 9. JCOP5.2 R2 Delivery Items (for R2.01.1 and R2.02.1)

Type	Name	Version
Product	NXP JCOP 5.2 on SN100.C58 Secure Element including software (JCOP5.2 OS, native applications and OS Update Component) that is identified by Platform ID.	see Table 12
Document	JCOP 5.2 R2 User Guidance Manual	see [13] (pdf)
Document	JCOP 5.2 R2 User Guidance Manual Addendum for SEMS API	see [14] (pdf)
Document	JCOP 5.2 R2 User Guidance Manual Addendum for CSP API	see [15] (pdf)

Table 10. JCOP5.2 R2 Delivery Items (for R2.03.1)

Type	Name	Version
Product	NXP JCOP 5.2 on SN100.C58 Secure Element including software (JCOP5.2 OS, native applications and OS Update Component) that is identified by Platform ID.	see Table 12
Document	JCOP 5.2 R2.03.1 User Guidance Manual	see [16] (pdf)
Document	JCOP 5.2 R2.03.1 User Guidance Manual Addendum for SEMS API	see [18] (pdf)
Document	JCOP 5.2 R2.03.1 User Guidance Manual Addendum for CSP API	see [17] (pdf)

Table 11. JCOP5.2 R3 Delivery Items (for R3.01.1)

Type	Name	Version
Product	NXP JCOP 5.2 on SN100.C58 Secure Element including software (JCOP5.2 OS, native applications and OS Update Component) that is identified by Platform ID.	see Table 12
Document	NXP. JCOP 5.2 R3.01.1, User Guidance Manual	see [19] (pdf)
Document	JCOP 5.2 R3.01.1 User Guidance Manual Addendum for SEMS API	see [21] (pdf)
Document	JCOP 5.2 R3.01.1 User Guidance Manual Addendum for CSP API	see [20] (pdf)

1.4 TOE Identification

The TOE platform can be identified by the JCOP Platform ID and the eUICC plugin ID, which is specific only to eUICC Domain. (see Table 12).

- The Platform ID can be obtained by using the GET PLATFORM IDENTIFIER command (see UGM section 1.3.1).
- The eUICC plugin ID can be obtained by using the GET EUICC PLUGIN VERSION command (see UGM section 1.3.2).

Note: The eUICC plugin may be tailored according to specific market or customer requirements. This Security Target identifies the plugin versions specific to this certificate. More than one plugin version may be valid for a product, due to varying market / customer requirements e.g. R3.01.1 product supports 2 different versions at the time of publication. Only one plugin version is installed at any time. Changes to the

plugin do not affect claims for the eSE domain. Customers should verify with NXP that the appropriate plugin version is installed for their specific requirements, as mentioned in the UGM.

Table 12. Product Identification

JCOP 5.2 Revision	Component	Identifier
R1.01.1	PID	N5C2M00261A70600
	eUICC plugin version	1.5.129
R2.01.1	PID	N5C2M0029E7D0600
	eUICC plugin version	1.5.146
R2.02.1	PID	N5C2M002A62D0600
	eUICC plugin version	1.5.148
R2.03.1	PID	N5C2M002CA640600
	eUICC plugin version	1.5.148
R3.01.1	PID	N5C2M002F8770600
	eUICC plugin version(s)	1.5.195 or 1.5.196

The Platform ID (PID) has the following form:

Nabcccxxxxxxyyzz

The "N" is constant, the other letters are variables. For a detailed description of these variables, please see Table 13.

Table 13. Platform ID Format (example R2.01.1)

Variable	Meaning	Value	Parameter Settings
a	Hardware Type	5	NFC hardware
b	JCOP OS Version	C	JCOP5.2
ccc	Non-Volatile Memory Size	2M0	2.0MB
ABCDEF	Build Number (hexadecimal)	029E7D	svn revision number - specific to each release
yy	Mask ID	06	Mask 6
zz	RFU	00	-

2 Conformance Claims

2.1 CC Conformance Claim

This Security Target claims to be conformant to the Common Criteria version 3.1:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, CCMB-2017-04-001, April 2017 [1].
- Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, CCMB-2017-04-002, April 2017 [2].
- Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, CCMB-2017-04-003, April 2017 [3].

For the evaluation the following methodology will be used:

- Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 5, CCMB-2017-04-004, April 2017 [4].

This Security Target claims to be CC Part 2 extended and CC Part 3 conformant. The extended Security Functional Requirements are defined in Chapter Section 6.

2.2 Package Claim

This Security Target claims conformance to the assurance package EAL5 augmented. The augmentation to EAL5 is AVA_VAN.5 “Advanced methodical vulnerability analysis”, ALC_DVS.2 “Sufficiency of security measures”, ASE_TSS.2 “TOE summary specification with architectural design summary”, and ALC_FLR.1 “Basic flaw remediation”.

2.3 PP Claim

The Security Target claims demonstrable conformance to the Java Card Protection Profile - Open Configuration [6]. The Java Card Protection Profile makes the use of Java Card RMI and "Management of External Memory (EXT-MEM)". The TOE does not support Java Card RMI nor "Extended Memory (EXT-MEM)". This ST is more restrictive than the PP [6] which Section 2.4 provides a rationale for.

The Security Target claims also demonstrable conformance to the eUICC for Consumer Devices Protection Profile (Base-PP only)[7].

The Security Target claims also strict conformance to the Cryptographic Service Provider Protection Profile [8].

2.4 Conformance Claim Rationale

2.4.1 TOE Type

The TOE type as stated in Section 1.2 of this ST corresponds to the TOE type of the PP as stated in Section 1.2 of [6] namely:

- A Java Card platform, implementing the Java Card Specification Version 3.0.5 [24][25] [23].
- An eUICC co-existing application, also underpinned by the Java Card and Global Platform Technologies, but accessible via separate, independent communications channels.

- An extended JavaCard package implementing the CSP specifications [43].

2.4.2 SPD Statement

2.4.2.1 JCOP

The SPD statement that is presented in Section 4 includes the threats as presented in the PPs [6] and [7], but also includes additional threats. These threats are:

- T.RND
- T.CONFID-UPDATE-IMAGE.LOAD
- T.INTEG-UPDATE-IMAGE.LOAD
- T.UNAUTH-LOAD-UPDATE-IMAGE
- T.INTERRUPT-OSU
- T.CONFIG
- T.COM_EXPLOIT
- T.LIFE_CYCLE
- T.UNAUTHORIZED_CARD_MNGT
- T.INTEG-APPLI-DATA[REFINED]
- T.ATTACK-COUNTER

The threat T.RND is taken from the Security IC PP [5].

The threats T.CONFID-UPDATE-IMAGE.LOAD, T.INTEG-UPDATE-IMAGE.LOAD, T.UNAUTH-LOAD-UPDATE-IMAGE and T.INTERRUPT-OSU are included for the OS Update which is additional functionality the PP allows.

The threat T.CONFIG is an additional threat to cover unauthorized modifications and read access of the configuration area in the TOE. It is an addition to the threats defined in the PP [6]. The threat T.ATTACK-COUNTER is included for the Restricted Mode which is additional functionality the PP allows. The threat T.COM_EXPLOIT is included to cover communication channels attacks and it is an addition to the threats in the PP [6].

The threat T.LIFE_CYCLE is included to cover content management attacks and it is an addition to the threats in the PP [6].

The threat T.UNAUTHORIZED_CARD_MNGT refines the threats T.INSTALL and T.DELETION from the PP [6].

The threat T.INTEG-APPLI-DATA[REFINED] refines the threat T.INTEG-APPLI-DATA in the PP [6].

Note that the threat T.EXE-CODE-REMOTE is not included, since the TOE does not support Java Card RMI. The Java Card Protection Profile [6] makes the use of Java Card RMI optional.

The SPD statement presented in Section 4, copies the OSP from the PP [6], and adds the following additional OSPs:

- OSP.PROCESS-TOE
- OSP.KEY-CHANGE
- OSP.SECURITY-DOMAINS

The OSP OSP.PROCESS-TOE is introduced for the pre-personalisation feature of the TOE and is an addition to the OSPs in PP [6]. The OSP OSP.KEY-CHANGE is introduced for the SD feature of the TOE and is an addition to the OSPs in PP [6]. The

OSP OSP.SECURITY-DOMAINS is introduced for the SD feature of the TOE and is an addition to the OSPs in PP [6].

The SPD statement includes two of the three assumptions from the PP [6]. The assumption A.Deletion is excluded. The Card Manager is part of the TOE and therefore the assumption is no longer relevant. Leaving out the assumption, makes the SPD of this ST more restrictive than the SPD in the PP [6]. As the Card Manager is part of the TOE, it is ensuring that the deletion of applets through the Card Manager is secure, instead of assuming that it is handled by the Card Manager in the environment of the TOE.

Besides the assumptions from the PP [6], five additional assumptions are added:

- A.PROCESS-SEC-IC
- A.USE_DIAG
- A.USE_KEYS
- A.APPS-PROVIDER
- A.VERIFICATION-AUTHORITY

The assumption A.PROCESS-SEC-IC is taken from the underlying certified Micro Controller [22], which is compliant to the Security IC PP [5].

The assumptions A.USE_DIAG and A.USE_KEYS are included because the Card Manager is part of the TOE and no longer part of the environment.

The assumptions A.APPS-PROVIDER and A.VERIFICATION-AUTHORITY are added because Security Domains from the GlobalPlatform Specification are introduced. All the applets and packages are signed by the APSD and the correctness is verified on the TOE by VASD before the package or applet is installed or loaded. A.APPS-PROVIDER and A.VERIFICATION-AUTHORITY are additions to PP [6] for card content management environment.

2.4.2.2 eUICC

The Security Problem Definition of the eUICC component is the same as in eUICC PP [7], no item have been added, removed or modified.

2.4.2.3 CSP

The Security Problem Definition of the CSP component is the same as in CSP PP [8], no item have been added, removed or modified.

2.4.3 Security Objectives Statement

2.4.3.1 JCOP

The statement of security objectives in the ST presented in Section 5 includes all security objectives as presented in the PP [6], but also includes a number of additional security objectives. These security objectives are:

- OT.IDENTIFICATION
- OT.RND
- OT.CONFID-UPDATE-IMAGE.LOAD
- OT.AUTH-LOAD-UPDATE-IMAGE
- OT.SECURE_LOAD_ACODE
- OT.SECURE_AC_ACTIVATION

- OT.TOE_IDENTIFICATION
- OT.CARD-CONFIGURATION
- OT.ATTACK-COUNTER
- OT.RESTRICTED-MODE
- OT.DOMAIN-RIGHTS
- OT.APPLI-AUTH
- OT.COMM_AUTH
- OT.COMM_INTEGRITY
- OT.COMM_CONFIDENTIALITY

The security objectives OT.IDENTIFICATION, OT.RND are part of the security objectives of the certified Micro Controller [5] (see also Section 1.3.2.1) which are also components of this composite certification. Therefore the security objective statement is equivalent to the PP [6] for these two security objectives. OT.IDENTIFICATION is also included for the pre-personalisation feature of the TOE, which is additional functionality the PP allows.

The security objective OT.CONFID-UPDATE-IMAGE.LOAD, OT.AUTH-LOAD-UPDATE-IMAGE, OT.SECURE_LOAD_ACODE, OT.SECURE_AC_ACTIVATION, OT.TOE_IDENTIFICATION are included for the OS Update which is additional functionality the PP allows. The security objectives OT.CARD-CONFIGURATION is included for the Config Applet which is additional functionality the PP allows. The security objectives OT.ATTACK-COUNTER and OT.RESTRICTED-MODE are included for the restricted mode which is additional functionality the PP allows. The security objectives OT.DOMAIN-RIGHTS, OT.APPLI-AUTH, OT.COMM_AUTH, OT.COMM_INTEGRITY, OT.COMM_CONFIDENTIALITY are objectives for the TOE as the GlobalPlatform API and the definitions for Secure Channel, Security Domains and Card Content Management are used from it.

The ST contains OE.APPLET, OE.VERIFICATION and OE.CODE-EVIDENCE from Security Objectives for the Operational Environment from [6]. Additionally, some of the Security Objectives for the Operational Environment from [6] are listed as TOE Security Objectives in this ST:

- OT.SCP.RECOVERY instead of OE.SCP.RECOVERY
- OT.SCP.SUPPORT instead of OE.SCP.SUPPORT
- OT.SCP.IC instead of OE.SCP.IC
- OT.CARD-MANAGEMENT instead of OE.CARD-MANAGEMENT

OT.SCP.RECOVERY, OT.SCP.SUPPORT, and OT.SCP.IC are objectives for the TOE as the Smart Card Platform belongs to the TOE for this evaluation. OT.CARD-MANAGEMENT is an objective for the TOE as the Card Manager belongs to the TOE for this evaluation. Moving objectives from the environment to the TOE, adds objectives to the TOE without changing the overall objectives. The statement of security objectives is therefore equivalent to the security objectives in the PP [6] to which conformance is claimed.

The security objectives OT.INSTALL, OT.LOAD, and OT.DELETION from the PP [6] are not included since these functionality and objectives are covered by the refined OT.CARD-MANAGEMENT.

Note that the objective OT.REMOTE is not included, since the TOE does not support Java Card RMI. The Java Card Protection Profile makes the use of Java Card RMI optional.

Note that the objective OT.EXT-MEM is not included, since the TOE does not support "Extended Memory (EXT-MEM)". The Java Card Protection Profile makes the use of "Extended Memory (EXT-MEM)" optional.

A part of the security objectives for the environment defined in the PP [6] has been included in this ST. The other part of security objectives for the environment, which is present in the PP [6], is used as part of the security objectives for the TOE in this ST. The ST also introduces eight additional security objectives for the environment. The additional objectives for the environment are:

- OE.USE_DIAG
- OE.USE_KEYS
- OE.PROCESS_SEC_IC
- OE.CONFID-UPDATE-IMAGE.CREATE
- OE.APPS-PROVIDER
- OE.VERIFICATION-AUTHORITY
- OE.KEY-CHANGE
- OE.SECURITY-DOMAINS

The security objective for the environment OE.PROCESS_SEC_IC is from the hardware platform (Micro Controller [5], see also Section 1.3.2.1) that is part of this composite product evaluation. Therefore the statement of security objectives for the environment is equivalent to the statement in the Security IC PP [5].

OE.USE_KEYS and OE.USE_DIAG are included because the Card Manager is part of the TOE and not a security objective for the environment as in PP [6].

The security objective for the environment OE.CONFID-UPDATE-IMAGE.CREATE is to cover the confidentiality during creation and transmission phase of D.UPDATE_IMAGE and therfore partly covers the threats introduced by the update mechanism which is additional functionality.

OE.APPS-PROVIDER and OE.VERIFICATION-AUTHORITY cover trusted actors which enable the creation, distribution and verification of secure applications. OE.KEY-CHANGE covers the switch to trusted keys for the AP. OE.SECURITY-DOMAINS covers the management of security domains in the context of the GlobalPlatform Specification.

The statement of security objectives for the environment is therefore considered to be equivalent to the security objectives in the PP [6] to which conformance is claimed.

2.4.3.2 eUICC

The Security Objectives for the TOE and its environment of the eUICC component is the same as in the eUICC PP [7] with some exclusions due to the overlap with the JCOP objectives defined in [6]:

- OE.IC.SUPPORT from eUICC PP [7] refines the objective OE.SCP.SUPPORT from the JCOP PP [6] with its own specific needs; it is then directly met by the coverage of the JCOP objective OE.SCP.SUPPORT.
- OE.IC.RECOVERY from eUICC PP [7] refines the objective OE.SCP.RECOVERY from the JCOP PP [6] with its own specific needs; it is then directly met by the coverage of the JCOP objective OE.SCP.RECOVERY.
- OE.RE.PPE-PPI from eUICC PP [7] is a request on the Runtime Environment and is met by the JCOP component objectives related to the threats T.DELETION and T.INSTALL defined in [6].

- OE.RE.SECURE-COMM from eUICC PP [7] is a request on the Runtime Environment and is met by the JCOP component objectives OT.FIREWALL and those related to the threats T.CONFID-APPLI-DATA and T.INTEG-APPLI-DATA defined in [6].
- OE.RE.API from eUICC PP [7] is a request on the Runtime Environment and is met by the JCOP component objectives related to the threats T.CONFID-JCS-CODE, T.INTEG-JCS-CODE, T.CONFID-JCS-DATA and T.INTEG-JCS-DATA defined in [6].
- OE.RE.DATA-CONFIDENTIALITY from eUICC PP [7] is a request on the Runtime Environment and is met by the JCOP component objectives related to the threat T.CONFID-APPLI-DATA defined in [6].
- OE.RE.DATA-INTEGRITY from eUICC PP [7] is a request on the Runtime Environment and is met by the JCOP component objectives related to the threats T.INTEG-APPLI-DATA, T.INTEG-APPLI-DATA.LOAD, T.INTEG-APPLI-CODE, T.INTEG-APPLI-CODE.LOAD defined in [6].
- OE.RE.CODE-EXE from eUICC PP [7] is a request on the Runtime Environment and is met by the JCOP component objectives related to the threats T.EXE-CODE.1, T.EXE-CODE.2 and T.NATIVE defined in [6].
- OE.RE.IDENTITY from eUICC PP [7] is a request on the Runtime Environment and is met by the JCOP component objectives related to the threats T.SID.1 and T.SID.2 defined in [6].
- OE.IC.PROOF_OF_IDENTITY from eUICC PP [7] is a request on the IC component and is met as described in Section 1.3.2.1.

2.4.3.3 CSP

The Security Objectives for the TOE and its environment of the CSP component is the same as in the CSP PP [8] with following exclusions due to the overlap with the JCOP objectives defined in [6]:

- OE.SecComm from CSP PP [8] is a request on the Runtime Environment and is met by the JCOP component objectives OT.FIREWALL and those related to the threats T.CONFID-APPLI-DATA and T.INTEG-APPLI-DATA defined in [6].

2.4.4 Security Functional Requirements Statement

2.4.4.1 JCOP

The Security Functional Requirements Statement copies most SFRs as defined in the PP [6], with the exception of a number of options. For the copied set of SFRs the ST is considered equivalent to the statement of SFRs in the PP [6]. Moreover as requested by the PP [6] the ST adds additional threats, objectives and SFRs to fully cover and describe additional security functionality implemented in the TOE.

The TOE restricts remote access from the CAD to the services implemented by the applets on the card to none, and as a result the SFRs concerning Java Card RMI (FDP_ACF.1[JCRMI], SFRs FDP_IFC.1/JCRMI, FDP_IFF.1/JCRMI, FMT_MSA.1/EXPORT, FMT_MSA.1/REM_REFS, FMT_MSA.3/JCRMI, FMT_SMF.1/JCRMI, FMT_REV.1/JCRMI, and FMT_SMR.1/JCRMI) are not included in the ST. In the PP [6] the use of the Java Card RMI is optional. The TOE does not implement Java Card RMI.

The TOE does not allow external memory access to the services implemented by the applets on the card, and as a result the SFRs concerning "Management of External Memory (EXT-MEM)" (FDP_ACC.1/EXT_MEM, FDP_ACF.1/EXT_MEM, FMT_MSA.1/EXT_MEM, FMT_MSA.3/EXT_MEM and FMT_SMF.1/EXT_MEM) are not included in

the ST. In the PP [6] the use of the "Management of External Memory (EXT-MEM)" is optional. The TOE does not implement "Management of External Memory (EXT-MEM)".

The SFR FDP_ITC.2/INSTALLER from the PP [6] is replaced by FDP_ITC.2[CCM] which enforces the Firewall access control policy and the Secure Channel Protocol information flow policy and which is more restrictive than the PACKAGE LOADING information flow control SFP from PP [6].

The set of SFRs that define the card content management mechanism CarG are partly replaced or refined and are considered to be equivalent or more restrictive because of the newly introduced SFPs:

- Security Domain access control policy
- Secure Channel Protocol information flow policy

These SFPs provide a concrete and more restrictive implementation of the PACKAGE LOADING information flow control SFP from PP [6] by following the information flow policy defined by Global latform specifications. The table below lists the SFRs from CarG of PP [6] and their corresponding refinements in this ST.

Table 14. CarG SFRs refinements

SFR from PP [6]	Refinement
FCO_NRO.2/CM	FCO_NRO.2[SC]
FDP_IFC.2/CM	FDP_IFC.2[SC]
FDP_IFF.1/CM	FDP_IFF.1[SC]
FDP_UIT.1/CM	FDP_UIT.1[CCM]
FIA_UID.1/CM	FIA_UID.1[SC]
FMT_MSA.1/CM	FMT_MSA.1[SC]
FMT_MSA.3/CM	FMT_MSA.3[SC]
FMT_SMF.1/CM	FMT_SMF.1[SC]
FMT_SMR.1/CM	FMT_SMR.1[SD]
FTP_ITC.1/CM	FTP_ITC.1[SC]

The following SFRs realize refinements of SFRs from PP [6] and add functionality to the TOE making the Security Functional Requirements Statement more restrictive than the PP [6]:

FDP_ROL.1[CCM], FPT_FLS.1[CCM] and FPT_PHP.3 realize additional security functionality for the card manager which is allowed by the PP [6].

The set of SFRs that define the security domains mechanism as specified by GlobalPlatform, realize refinements of SFRs from PP [6] (see above Table 14) and additional security functionality which is allowed by the PP [6]. This set of SFRs comprise FDP_ACC.1[SD], FDP_ACF.1[SD], FMT_MSA.1[SD], FMT_MSA.3[SD], FMT_SMF.1[SD], and FMT_SMR.1[SD].

The set of SFRs that define the secure channel mechanism as specified by GlobalPlatform, realize refinements of SFRs from PP [6] (see above Table 14) and additional security functionality which is allowed by the PP [6]. This set of SFRs comprise FCO_NRO.2[SC], FDP_IFC.2[SC], FDP_IFF.1[SC], FMT_MSA.1[SC], FMT_MSA.3[SC], FMT_SMF.1[SC], FIA_UID.1[SC], FIA_UAU.1[SC], FIA_UAU.4[SC], and FTP_ITC.1[SC].

The SFRs FAU_SAS.1[SCP], FIA_AFL.1[PIN] and FCS_RNG.1 realize additional security functionality which is allowed by the PP [6].

The set of SFRs that define the Config Applet realize additional security functionality, which is allowed by the PP [6]. This set of SFRs comprise FDP_IFC.2[CFG], FDP_IFF.1[CFG], FIA_UID.1[CFG], FMT_MSA.1[CFG], FMT_MSA.3[CFG], FMT_SMF.1[CFG], FMT_SMR.1[CFG] The set of SFRs that define the OS Update realize additional security functionality, which is allowed by the PP [6]. This set of SFRs comprise FDP_IFC.2[OSU], FDP_IFF.1[OSU], FMT_MSA.3[OSU], FMT_MSA.1[OSU], FMT_SMR.1[OSU], FMT_SMF.1[OSU], FIA_UID.1[OSU], FIA_UAU.1[OSU], FIA_UAU.4[OSU] and FPT_FLS.1[OSU].

The set of SFRs that define the Restricted Mode realize additional security functionality, which is allowed by the PP [6]. This set of SFRs comprise FDP_ACC.2[RM], FDP_ACF.1[RM], FMT_MSA.3[RM], FMT_MSA.1[RM], FMT_SMF.1[RM], FIA_UID.1[RM] and FIA_UAU.1[RM].

2.4.4.2 eUICC

The Security Functional Requirements for the eUICC component are the same as in eUICC PP [7], none have been added, removed or modified.

2.4.4.3 CSP

The Security Functional Requirements for the CSP component are the same as in CSP PP [8] with some exclusions due to the overlap with the JCOP PP [6]:

- Common cryptographic SFRs: SFRs FCS_RNG.1 and FCS_CKM.4
- Common self-protection requirements: FPT_PHP.3

The confidentiality of stored data by encryption mechanism is handled at the hardware level as described in [22]; SFRs FDP_SDC.1 and related SFRs FCS_CKM.1[SDEK] and FCS_COP.1[SDE] are then also excluded due to this overlap.

In SFR FTP_TST.1, the requirements that a test suite has to be run "at the request of the authorised user" is not implemented by the issuance of a dedicated command; however, at the execution of any command invoked by users, regular integrity checks by are performed by the underlying JavaCard platform and hardware platform (memory integrity verification, control flow, etc.).

In SFR FDP_ACF.1.2[UCP], the statement "Version Number of the Update Code Package is equal or higher than the Version Number of the TSF" is hanlded by a requirement into the UGM [12]

The following SFRs names are extended with the "[CSP]" iterations to identify them as part of the CSP component: FIA_AFL.1, FIA_ATD.1, FIA_UID.1, FIA_UAU.1, FIA_UAU.5, FIA_UAU.6, FIA_USB.1, FMT_MOF.1, FMT_SMF.1, FMT_SMR.1, FMT_MSA.2, FMT_MTD.3, FMT_SAE, FPT_FLS.1, FTP_ITC.1, FPT_TST.1, FRU_FLT.2

In remaining SFRs, any item related to the following mechanisms are not supported (as authorized by the CSP PP [8]):

- Clustering
- Time service
- Time stamps
- Audit

Concerning the SFRs dependency, only the following differences exist:

- FCS_COP.1[VDSUCP]: the import of UCP signature verification key is done during manufacturing.
- FCS_COP.1.1[DecUCP]: the import of UCP decryption key is done during manufacturing.

3 Security Aspects

This chapters described only the Security Aspects which have been added to the JCOP PP [6].

3.1 Confidentiality

Table 15.

SA.CONFID-UPDATE-IMAGE	**Confidentiality of Update Image** The update image must be kept confidential. This concerns the non disclosure of the update image in transit to the card.

3.2 Integrity

Table 16.

SA.INTEG-UPDATE-IMAGE	**Integrity of Update Image** The update image must be protected against unauthorized modification. This concerns the modification of the image in transit to the card.

3.3 Config Applet

Table 17.

SA.CONFIG-APPLET	**Config Applet** The Config Applet is a JCOP functionality which allows to: • Read and modify configuration items in the configuration area of the TOE, • Disable Access to configuration item.

3.4 OS Update

Table 18.

SA.OSU	**OS Update** The UpdaterOS allows to update JCOP5.2 OS and the UpdaterOS itself. It ensures that only valid updates can be installed on the TOE.

3.5 Restricted Mode

Table 19.

SA.RM	**Restricted Mode** If the Attack Counter reaches its limit the TOE goes into Restricted Mode. In this mode it is possible to perform a limited set of functions, like authenticate against the ISD, reset the Attack Counter or read logging information.

4 Security Problem Definition (ASE_SPD)

4.1 JCOP

The Security Problem Definition for the JCOP component of the TOE adds and refines items regarding the Security Problem Definition described in the JavaCard PP [6].

The following sections described only additional and refined items.

4.1.1 JCOP Threats

4.1.1.1 Integrity

Table 20.

T.INTEG-APPLI-DATA [REFINED]	**Integrity of Application Data** The attacker executes an application to alter (part of) another application's data. See SA.INTEG-APPLI-DATA for details. Directly threatened asset(s): D.APP_I_DATA, D.PIN, D.APP_KEYS, D.ISD_KEYS, D.VASD_KEYS and S.APSD_KEYS. This threat is a refinement of the Threat T.INTEG-APPLI-DATA from [6].

4.1.1.2 Card Management

Table 21.

T.UNAUTHORIZED_CARD_MNGT	**Unauthorized Card Management** The attacker performs unauthorized card management operations (for instance impersonates one of the actor represented on the card) in order to take benefit of the privileges or services granted to this actor on the card such as fraudulent: • load of a package file • installation of a package file • extradition of a package file or an applet • personalization of an applet or a Security Domain • deletion of a package file or an applet • privileges update of an applet or a Security Domain Directly threatened asset(s): D.ISD_KEYS, D.APSD_KEYS, D.APP_C_DATA, D.APP_I_DATA, D.APP_CODE, D.SEC_DATA, and D.CARD_MNGT_DATA (any other asset may be jeopardized should this attack succeed, depending on the virulence of the installed application). This security objective is a refinement of the Threats T.INSTALL and T.DELETION from [6].
T.COM_EXPLOIT	**Communication Channel Remote Exploit** An attacker remotely exploits the communication channels established between a third party and the TOE in order to modify or disclose confidential data. All assets are threatened.
T.LIFE_CYCLE	**Life Cycle** An attacker accesses to an application outside of its expected availability range thus violating irreversible life cycle phases of the application (for instance, an attacker repersonalizes the application). Directly threatened asset(s): D.APP_I_DATA, D.APP_C_DATA, and D.CARD_MNGT_DATA.

4.1.1.3 Random Numbers

Table 22.

T.RND	**Deficiency of Random Numbers** An attacker may predict or obtain information about random numbers generated by the TOE for instance because of a lack of entropy of the random numbers provided. An attacker may gather information about the produced random numbers which might be a problem because they may be used for instance to generate cryptographic keys. Here the attacker is expected to take advantage of statistical properties of the random numbers generated by the TOE without specific knowledge about the TOE's generator. Malfunctions or premature ageing are also considered which may assist in getting information about random numbers.

4.1.1.4 Config Applet

Table 23.

T.CONFIG	**Unauthorized configuration** The attacker tries to change configuration items without authorization. Directly threatened asset(s): D.CONFIG_ITEM.

4.1.1.5 OS Update

Table 24.

T.CONFID-UPDATE-IMAGE.LOAD	**Confidentiality of Update Image - Load** The attacker discloses (part of) the image used to update the TOE in the field while the image is transmitted to the card for installation. See SA.CONFID-UPDATE-IMAGE for details. Directly threatened asset(s): D.UPDATE_IMAGE, D.JCS_CODE, and D.JCS_DATA.
T.UNAUTH-LOAD-UPDATE-IMAGE	**Load unauthorized version of Update Image** The attacker tries to upload an unauthorized Update Image. Directly threatened asset(s): D.JCS_CODE, D.JCS_DATA, D.UPDATE_IMAGE.
T.INTEG-UPDATE-IMAGE.LOAD	**Integrity of Update Image - Load** The attacker modifies (part of) the image used to update the TOE in the field while the image is transmitted to the card for installation. See SA.INTEG-UPDATE-IMAGE for details. Directly threatened asset(s): D.UPDATE_IMAGE, D.JCS_CODE, and D.JCS_DATA.
T.INTERRUPT-OSU	**OS Update procedure interrupted** The attacker tries to interrupt the OS Update procedure (Load Phase through activation of additional code) leaving the TOE in a partially functional state. Directly threatened asset(s): D.JCS_CODE, D.JCS_DATA, D.UPDATE_IMAGE, D.TOE_IDENTIFIER.

4.1.1.6 Restricted Mode

Table 25.

T.ATTACK-COUNTER	**Modification of the Attack Counter** The attacker tries to modify the attack counter without authorization. Directly threatened asset: D.ATTACK_COUNTER.

4.1.2 JCOP related Organisational Security Policies

OSP.PROCESS-TOE **Identification of the TOE**

An accurate identification must be established for the TOE. This requires that each instantiation of the TOE carries this identification.

OSP.KEY-CHANGE **Security Domain Keys Change**

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

OSP.SECURITY-DOMAINS **Security Domains**

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

4.1.3 JCOP related Assumptions

A.USE_DIAG **Usage of TOE's Secure Communication Protocol by OE**

It is assumed that the operational environment supports and uses the secure communication protocols offered by the TOE.

A.USE_KEYS **Protected Storage of Keys Outside of TOE**

It is assumed that the keys which are stored outside the TOE and which are used for secure communication and authentication between Smart Card and terminals are protected for confidentiality and integrity in their own storage environment. This is especially true for D.APSD_KEYS, D.ISD_KEYS, and D.VASD_KEYS.

Info: This is to assume that the keys used in terminals or systems are correctly protected for confidentiality and integrity in their own environment, as the disclosure of such information which is shared with the TOE but is not under the TOE control, may compromise the security of the TOE.

A.PROCESS-SEC-IC **Protection during Packaging, Finishing and Personalisation**

It is assumed that security procedures are used after delivery of the TOE by the TOE Manufacturer up to delivery to the end consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that the Phases after TOE Delivery are assumed to be protected appropriately. The assets to be protected are: The information and material produced and/or processed by the Security IC Embedded Software Developer in Phase 1 and by the Composite Product Manufacturer can be grouped as follows:

- the Security IC Embedded Software including specifications, implementation and related documentation,
- pre-personalisation and personalisation data including specifications of formats and memory areas, test related data,
- the User Data and related documentation, and
- material for software development support

as long as they are not under the control of the TOE Manufacturer.

A.APPS-PROVIDER **Application Provider**

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

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

A.VERIFICATION-AUTHORITY	**Verification Authority** The VA is a trusted actor who is able to verify bytecode of an application loaded on the card, guarantee and generate the digital signature attached to an application and ensure that its public key for verifying the application signature is on the TOE. *Info*: As a consequence, it guarantees the success of the application validation upon loading.

4.2 eUICC

The Securiity Problem Definition for the JCOP component of the TOE is strictly compliant with the Security Problem Definition described in the eUICC PP [7].

4.3 CSP

The Securiity Problem Definition for the JCOP component of the TOE is strictly compliant with the Security Problem Definition described in the CSP PP [8].

5 Security objectives

5.1 Security Objectives for the TOE

5.1.1 JCOP

The Security Objectives for the JCOP component of the TOE adds and refines items regarding the Security Objectives for the TOE described in the JCOP PP [6].

The following sections described only additional and refined items.

5.1.1.1 Smart Card Platform

Table 26.

OT.SCP.IC	**IC Physical Protection** The SCP shall provide all IC security features against physical attacks. This security objective for the environment refers to the point (7) of the security aspect SA.SCP. AppNote: The Security Objectives from [6] for the environment OE.SCP.RECOVERY, OE.SCP.SUPPORT, and OE.SCP.IC are listed as TOE Security Objectives (OT.SCP.RECOVERY, OT.SCP.SUPPORT, and OT.SCP.IC) for the TOE in this section as the Smart Card Platform belongs to the TOE for this evaluation.
OT.SCP.RECOVERY	**SCP Recovery** 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. This security objective for the environment refers to the security aspect SA.SCP AppNote: The Security Objectives from [6] for the environment OE.SCP.RECOVERY, OE.SCP.SUPPORT, and OE.SCP.IC are listed as TOE Security Objectives (OT.SCP.RECOVERY, OT.SCP.SUPPORT, and OT.SCP.IC) for the TOE in this section as the Smart Card Platform belongs to the TOE for this evaluation.
OT.SCP.SUPPORT	**SCP Support** The SCP shall support the TSFs of the TOE. This security objective refers to the security aspects 2, 3, 4 and 5 of SA.SCP AppNote: The Security Objectives from [6] for the environment OE.SCP.RECOVERY, OE.SCP.SUPPORT, and OE.SCP.IC are listed as TOE Security Objectives (OT.SCP.RECOVERY, OT.SCP.SUPPORT, and OT.SCP.IC) for the TOE in this section as the Smart Card Platform belongs to the TOE for this evaluation.
OT.IDENTIFICATION	**TOE identification** The TOE must provide means to store Initialization Data and Pre-personalization Data in its non-volatile memory. The Initialization Data (or parts of them) are used for TOE identification.

5.1.1.2 Random Numbers

Table 27.

OT.RND	**Quality of random numbers** The TOE will ensure the cryptographic quality of random number generation. For instance random numbers shall not be predictable and shall have sufficient entropy. The TOE will ensure that no information about the produced random numbers is available to an attacker since they might be used for instance to generate cryptographic keys.

5.1.1.3 OS Update Mechanism

Table 28.

OT.CONFID-UPDATE-IMAGE.LOAD	**Confidentiality of Update Image - Load** The TOE shall ensure that the encrypted image transferred to the device is not disclosed during the installation. The keys used for decrypting the image shall be kept confidential.
OT.AUTH-LOAD-UPDATE-IMAGE	**Authorization of Update Image - Load** The TOE shall ensure that it is only possible to load an authorized image.

The following Security Objectives have been added to comply to JIL "Security requirements for post-delivery code loading" [9].

Table 29.

OT.SECURE_LOAD_ACODE	**Secure loading of the Additional Code** The Loader of the Initial TOE shall check an evidence of authenticity and integrity of the loaded Additional Code. The Loader enforces that only the allowed version of the Additional Code can be loaded on the Initial TOE. The Loader shall forbid the loading of an Additional Code not intended to be assembled with the Initial TOE. During the Load Phase of an Additional Code, the TOE shall remain secure.
OT.SECURE_AC_ACTIVATION	**Secure activation of the Additional Code** Activation of the Additional Code and update of the Identification Data shall be performed at the same time in an Atomic way. All the operations needed for the code to be able to operate as in the Final TOE shall be completed before activation. If the Atomic Activation is successful, then the resulting product is the Final TOE, otherwise (in case of interruption or incident which prevents the forming of the Final TOE), the Initial TOE shall remain in its initial state or fail secure.
OT.TOE_IDENTIFICATION	**Secure identification of the TOE** The Identification Data identifies the Initial TOE and Additional Code. The TOE provides means to store Identification Data in its non-volatile memory and guarantees the integrity of these data. After Atomic Activation of the Additional Code, the Identification Data of the Final TOE allows identifications of Initial TOE and Additional Code. The user shall be able to uniquely identify Initial TOE and Additional Code(s) which are embedded in the Final TOE.

5.1.1.4 Config Applet

Table 30.

OT.CARD-CONFIGURATION	**Card Configuration** The TOE shall ensure that the customer can only configure customer configuration items and that NXP can configure customer and NXP configuration items. Additionally, the customer can only disable the customer configuration and NXP can disable customer and NXP configuration.

5.1.1.5 Restricted Mode

Table 31.

OT.ATTACK-COUNTER	**Attack Counter** The TOE shall ensure that the Attack Counter can only be reset by the ISD or by application of an ECC signed token.
OT.RESTRICTED-MODE	**Restricted Mode** The TOE shall ensure that in Restricted Mode all operations return an error except for the limited set of commands that are allowed by the TOE when in Restricted Mode.

5.1.1.6 Applet Management

Table 32.

OT.APPLI-AUTH	**Application Authentication** The card manager shall enforce the application security policies established by the card issuer by requiring application authentication during application loading on the card. This security objective is a refinement of the Security Objective OT.LOAD from [6]. AppNote: Each application loaded onto the TOE has been signed by a VA. The VA will guarantee that the security policies established by the card issuer on applications are enforced. For example this authority (DAP) or a third party (Mandated DAP) can be present on the TOE as a Security Domain whose role is to verify each signature at application loading.
OT.DOMAIN-RIGHTS	**Domain Rights** The Card issuer shall not get access or change personalized AP Security Domain keys which belong to the AP. Modification of a Security Domain keyset is restricted to the AP who owns the security domain. AppNote: APs have a set of keys that allows them to establish a secure channel between them and the platform. These keys sets are not known by the TOE issuer. The security domain initial keys are changed before any operation on the SD (OE.KEY-CHANGE).
OT.COMM_AUTH	**Communication Mutual Authentication** The TOE shall authenticate the origin of the card management requests that the card receives, and authenticate itself to the remote actor.
OT.COMM_INTEGRITY	**Communication Request Integrity** The TOE shall verify the integrity of the card management requests that the card receives.
OT.COMM_CONFIDENTIALITY	**Communication Request Confidentiality** The TOE shall be able to process card management requests containing encrypted data.

5.1.2 eUICC

The Security Objectives for the eUICC component of the TOE is strictly compliant with the Security Objectives for the TOE described in the eUICC PP [7].

5.1.3 CSP

The Security Objectives for the CSP component of the TOE is strictly compliant with the Security Objectives for the TOE described in the CSP PP [8].

5.2 Security Objectives for the Environment

5.2.1 JCOP

The Security Objectives for the environment of the JCOP component of the TOE adds items regarding the Security Objectives for the Environment described in the JCOP PP [6].

The following sections described only additional and refined items.

OE.APPS-PROVIDER	**Application Provider** The AP shall be a trusted actor that provides applications. The AP is responsible for its security domain keys.
OE.VERIFICATION-AUTHORITY	**Verification Authority** The VA should be a trusted actor who is able to verify bytecode of an application loaded on the card, guarantee and generate the digital signature attached to an application and ensure that its public key for verifying the application signature is on the TOE.
OE.KEY-CHANGE	**Security Domain Key Change** The AP must change its security domain initial keys before any operation on it.
OE.SECURITY-DOMAINS	**Security Domains** Security domains can be dynamically created, deleted and blocked during usage phase in post-issuance mode.
OE.USE_DIAG	**Secure TOE communication protocols** Secure TOE communication protocols Secure TOE communication protocols shall be supported and used by the environment.
OE.USE_KEYS	**Protection of OPE keys** During the TOE usage, the terminal or system in interaction with the TOE, shall ensure the protection (integrity and confidentiality) of their own keys by operational means and/or procedures.
OE.PROCESS_SEC_IC	**Protection during composite product manufacturing** Security procedures shall be used after TOE Delivery up to delivery to the end-consumer to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use). This means that Phases after TOE Delivery up to the end of Phase 6 must be protected appropriately.

OE.CONFID-UPDATE-IMAGE.CREATE	**Confidentiality of Update Image - CREATE** The off-card Update Image Creator ensures that the image is signed and transferred encrypted to the device and is not disclosed during the creation and transfer. The keys used for signing and encrypting the image are kept confidential.

5.2.2 eUICC

The Security Objectives for the Environment of the eUICC component are the same as the Security Objectives for the Environment described in the eUICC PP [7] with the exclusions justified in Section 2.4.3.2.

5.2.3 CSP

The Security Objectives for the Environment of the CSP component are the same as Security Objectives for the Environment described in the CSP PP [8] with the exclusion justified in Section 2.4.3.3.

5.3 Security Objectives Rationales

5.3.1 JCOP

The following rationales of Security Objectives for the JCOP component only covers the modifications regarding the JCOP PP [6] due to additions and refinements in Security Problem Definition and Security Objectives.

5.3.1.1 Threats

5.3.1.1.1 Confidentiality

5.3.1.1.1.1 T.CONFID-UPDATE-IMAGE.LOAD

Table 33.

Objective	Rationale
OT.CONFID-UPDATE-IMAGE.LOAD	Counters the threat by ensuring the confidentiality of D.UPDATE_IMAGE during installing it on the TOE.
OE.CONFID-UPDATE-IMAGE.CREATE	Counters the threat by ensuring that the D.UPDATE_IMAGE is not transfered in plain and that the keys are kept secret.

5.3.1.1.2 Integrity

5.3.1.1.2.1 T.INTEG-UPDATE-IMAGE.LOAD

Table 34.

Objective	Rationale
OT.SECURE_LOAD_ACODE	Counters the threat directly by ensuring the authenticity and integrity of D.UPDATE_IMAGE.

5.3.1.1.3 Card Management

5.3.1.1.3.1 T.UNAUTHORIZED_CARD_MNGT

Table 35.

Objective	Rationale
OT.CARD-MANAGEMENT	Contributes to counter this threat by controlling the access to card management functions such as the loading, installation, extradition or deletion of applets.
OT.DOMAIN-RIGHTS	Contributes to counter this threat by restricting the modification of an AP security domain keyset to the AP who owns it.
OT.COMM_AUTH	Contributes to counter this threat by preventing unauthorized users from initiating a malicious card management operation.
OT.COMM_INTEGRITY	Contributes to counter this threat by protecting the integrity of the card management data while it is in transit to the TOE.
OT.APPLI-AUTH	Counters this threat by ensuring that the loading of a package is safe.

5.3.1.1.3.2 T.COM_EXPLOIT

Table 36.

Objective	Rationale
OT.COMM_AUTH	Contributes to counter this threat by preventing unauthorized users from initiating a malicious card management operation.
OT.COMM_INTEGRITY	Contributes to counter this threat by protecting the integrity of the card management data while it is in transit to the TOE.
OT.COMM_CONFIDENTIALITY	Contributes to counter this threat by preventing from disclosing encrypted data transiting to the TOE.

5.3.1.1.3.3 T.LIFE_CYCLE

Table 37.

Objective	Rationale
OT.CARD-MANAGEMENT	Contributes to counter this threat by controlling the access to card management functions such as the loading, installation, extradition or deletion of applets.
OT.DOMAIN-RIGHTS	Contributes to counter this threat by restricting the use of an AP security domain keysets, and thus the management of the applications related to this SD, to the AP who owns it.

5.3.1.1.4 Random Numbers

5.3.1.1.4.1 T.RND

Table 38.

Objective	Rationale
OT.RND	Counters the threat by ensuring the cryptographic quality of random number generation. For instance random numbers shall not be predictable and shall have sufficient entropy. Furthermore, the TOE ensures that no information about the produced random numbers is available to an attacker.

5.3.1.1.5 Config Applet

5.3.1.1.5.1 T.CONFIG

Table 39.

Objective	Rationale
OT.CARD-CONFIGURATION	Counters the threat by ensuring that the customer can only read and write customer configuration items using the Customer Configuration Token and NXP can read and write configuration items using the NXP Configuration Token generation key. If access is disabled configuration items can not be read or written.

5.3.1.1.6 OS Update

5.3.1.1.6.1 T.UNAUTH-LOAD-UPDATE-IMAGE

Table 40.

Objective	Rationale
OT.SECURE_LOAD_ACODE	Counters the threat directly by ensuring that only authorized (allowed version) images can be installed.
OT.AUTH-LOAD-UPDATE-IMAGE	Counters the threat directly by ensuring that only authorized (allowed version) images can be loaded.

5.3.1.1.6.2 T.INTERRUPT-OSU

Table 41.

Objective	Rationale
OT.SECURE_LOAD_ACODE	Counters the threat directly by ensuring that the TOE remains in a secure state after interruption of the OS Update procedure (Load Phase).
OT.TOE_IDENTIFICATION	Counters the threat directly by ensuring that D.TOE_IDENTIFICATION is only updated after successful OS Update procedure.
OT.SECURE_AC_ACTIVATION	Counters the threat directly by ensuring that the update OS is only activated after successful (atomic) OS Update procedure.

5.3.1.1.7 Restricted Mode

5.3.1.1.7.1 T.ATTACK-COUNTER

Table 42.

Objective	Rationale
OT.ATTACK-COUNTER	Counters the threat by ensuring that only the ISD can reset the Attack Counter.
OT.RESTRICTED-MODE	Counters the threat by ensuring that only the ISD can reset the Attack Counter.

5.3.1.1.8 Miscellaneous

5.3.1.1.8.1 T.PHYSICAL

Table 43.

Objective	Rationale
OT.SCP.IC	Counters phyiscal attacks. Physical protections rely on the underlying platform and are therefore an environmental issue.
OT.RESTRICTED-MODE	Contributes to counter the threat by ensuring that if the limit of the Attack Counter is reached only limited functionality is available.

5.3.1.2 Assumptions

5.3.1.2.1 A.USE_DIAG

Table 44.

Objective	Rationale
OE.USE_DIAG	Directly upholds this assumption.

5.3.1.2.2 A.USE_KEYS

Table 45.

Objective	Rationale
OE.USE_KEYS	Directly upholds this assumption.

5.3.1.2.3 A.PROCESS-SEC-IC

Table 46.

Objective	Rationale
OE.PROCESS_SEC_IC	Directly upholds this assumption.

5.3.1.2.4 A.APPS-PROVIDER

Table 47.

Objective	Rationale
OE.APPS-PROVIDER	Directly upholds this assumption.

5.3.1.2.5 A.VERIFICATION-AUTHORITY

Table 48.

Objective	Rationale
OE.VERIFICATION-AUTHORITY	Directly upholds this assumption.

5.3.1.3 Organizational Security Policies

5.3.1.3.1 OSP.PROCESS-TOE

Table 49.

Objective	Rationale
OT.IDENTIFICATION	Enforces this organisational security policy by ensuring that the TOE can be uniquely identified.

5.3.1.3.2 OSP.KEY-CHANGE

Table 50.

Objective	Rationale
OE.KEY-CHANGE	Enforces the OSP by ensuring that the initial keys of the security domain are changed before any operation on them are performed.

5.3.1.3.3 OSP.SECURITY-DOMAINS

Table 51.

Objective	Rationale
OE.SECURITY-DOMAINS	Enforces the OSP by dynamically create, delete, and block the security domain during usage phase in post-issuance mode.

5.3.2 eUICC

The rationales of applicable Security Objectives for the eUICC component and for its Environment are strictly the same in the eUICC PP [7].

5.3.3 CSP

The rationales of applicable Security Objectives for the CSP component and its environment are strictly the same in the CSP PP [8].

6 Extended Components Definition

6.1 JCOP

Following extended components have been taken with no modification from the claimed JCOP PP [6]:

- FCS_RNG.

Additionally, the following extended components have been taken with no modification from the Smartcard IC Platform PP [5]:

- FAU_SAS.1

6.2 eUICC

Following extended components have been taken with no modification from the claimed eUICC PP [7]:

- FIA_API, FPT_EMS (renamed FPT_EMSEC) and FCS_RNG.

6.3 CSP

Following extended components have been taken with no modification from the claimed CSP PP [8]:

- FCS_RNG, FCS_CKM.5, FIA_API, FPT_TCT, FPT_TIT, FPT_ISA, FPT_ESA, FDP_SDC.

7 Security Requirements (ASE_REQ)

7.1 Security Functional Requirements

7.1.1 JCOP

The Security Functional Requirements for the JCOP component of the TOE implements all SFRs of the the JCOP PP [6]; however some are refined and some are added (see Conformance Claim Rationale).

In the following, only modified or added items regarding the JCOP PP [6] are described.

7.1.1.1 SFRs content items definitions

Additional groups used for readability purposes are defined:

Table 52. Requirement Groups

Group	Description
Configuration	SFRs related to NXP Proprietary product configuration feature.
OS UPdate	SFRs related to NXP Proprietary OS Update feature
Restricted Mode	SFRs related to NXP Proprietary Restricted Mode.

Additional subjects acting on behalf of TOE users are defined:

Table 53. Java Card Subject Descriptions

Subjects	Descriptions
S.SD	A GlobalPlatform Security Domain representing on the card a off-card entity. This entity can be the Issuer, an Application Provider, the Controlling Authority or the Verification Authority.
S.OSU	OSU provides secure functionality to update the TOE operating system with an image created by a trusted off-card entity (S.UpdateImageCreator)
S.UpdateImageCreator	The off-card Update Image Creator ensures that the image is signed and transferred encrypted to the device and is not disclosed during the creation and transfer. The keys used for signing and encrypting the image are kept confidential.
S.Customer	The subject that has the Customer Configuration Token.
S.NXP	The subject that has the NXP Configuration Token generation key.
S.ConfigurationMechanism	On card entity which can read and write configuration items.

No additional objects are defined.

Additional security attributes linked to subjects, objects and information are defined:

Table 54. Security attribute description

Security attributes	Description
Attack Counter	Attack Counter

Security attributes	Description
Current Sequence Number	The current number of a valid OS installed on the TOE or current number of a OS update step during update process.
Final Sequence Number	The sequence number which is reached after completing the update process. This is uniquely linked to the JCOP version of the final TOE.
Image Type	Type of D.UPDATE_IMAGE. Can be either Upgrade, Self Update or Downgrade.
Reference Sequence Number	Is the sequence number which the TOE has before the update process is started. This is uniquely linked to the JCOP version of the initial TOE.
Address Space	Accessible memory portion.
Verification Key	Key to verify integrity of D.UPDATE_IMAGE.
Decryption Key	Key for decrypting D.UPDATE_IMAGE.
Customer Configuration Token generation key	The customer key to generate tokens for product configuration.
NXP Configuration Token generation key	The NXP key to generate tokens for product configuration.
Attack Counter Token Key	The key to generate tokens for Attack Counter Reset.
NXP Configuration Access	The NXP Configuration Access can either be enabled or disabled.
Customer Configuration Access	The Customer Configuration Access can either be enabled or disabled.
Access privilege	For each configuration item the access privilege attribute defines who (Customer and/or NXP) is allowed to read/write the item.
Key Set	Key Set for Secure Channel.
Received Sequence Number	Sequence number of the uploaded D.UPDATE_IMAGE.
Security Level	Secure Communication Security Level defined in Section 10.6 of [26].
Secure Channel Protocol	Secure Channel Protocol version used.
Session Key	Secure Channel's session key.
Sequence Counter	Secure Channel Session's Sequence Counter.
ICV	Secure Channel Session's ICV.
CPU Mode	The execution mode of the CPU. Can be either Application Privileged Mode, Application Unprivileged Mode and Shared Mode. The modes Service Privileged and Service Unprivileged are reserved to the Security Software execution.
MMU Segment Table	Defines the memory areas which can be accessed for read/write/ execute.
Special Function Registers	Special Function Registers allow to set operation modes of functional blocks of the hardware.
Card Life Cycle	Defined in Section 5.1.1 of [26].
Privileges	Defined in Section 6.6.1 of [26].

Security attributes	Description
Life-cycle Status	Defined in Section 5.3.2 of v.

Additional operations are defined:

Table 55. Operation Description

Operations	Description
OP.READ_CONFIG_ ITEM	Reading a Config Item from the configuration area.
OP.MODIFY_ CONFIG_ITEM	Writing of a Config Item.
OP.USE_CONFIG_ ITEM	Operational usage of Config Items by subjects inside the TOE.
OP.TRIGGER_ UPDATE	APDU Command that initializes the OS Update procedure.

7.1.1.2 COREG_LC Security Functional Requirements

The list of SFRs of this category are taken from [6].

7.1.1.2.1 Firewall policy

The following table provides the assignments and/or selections of related SFRs taken from the JCOP PP [6]:

Table 56.

SFR ID	Selection / Assignment text	Selection / Assignment value
FDP_IFF.1.3/ JCVM	[assignment: additional information flow control SFP rules]	no additional information flow control SFP rules
FDP_IFF.1.4/ JCVM	[assignment: rules, based on security attributes, that explicitly authorise information flows]	none
FDP_IFF.1.5/ JCVM	[assignment: rules, based on security attributes, that explicitly authorise information flows]	none

7.1.1.2.2 Application Programming Interface

The following table provides the assignments and/or selections of related SFRs taken from the JCOP PP [6]:

Table 57.

SFR ID	Selection / Assignment text	Selection / Assignment value
FCS_CKM.1.1/	[assignment: cryptographic key generation algorithm]	JCOP RNG

SFR ID	Selection / Assignment text	Selection / Assignment value
	[assignment: cryptographic key sizes]	DES: Key lengths - LENGTH_DES3_2KEY, LENGTH_DES3_3KEY bit, AES: Key lengths - LENGTH_AES_128, LENGTH_AES_192, LENGTH_AES_256 bit RSA-CRT and RSA: Any length that is a multiple of 32 from 512 to 2048 bits, ECC: Key lengths - Any length from 128 to 528 bits
	[assignment: list of standards]	[45]
FCS_CKM.4.1/	[assignment: cryptographic key destruction method]	physically overwriting the keys in a randomized manner]
	[assignment: list of standards]	none
FCS_COP.1.1 [GCM]	[assignment: list of cryptographic operations]	decryption and encryption
	[assignment: cryptographic algorithm]	AES in GCM mode
	[assignment: cryptographic key sizes]	128 bits
	[assignment: list of standards]	FIPS 197 [47], Recommendation for BlockCipher [52]
FCS_COP.1.1 [TriplerDES]	[assignment: list of cryptographic operations]	decryption and encryption
	[assignment: cryptographic algorithm]	• ALG_DES_CBC_ISO9797_M1 • ALG_DES_CBC_ISO9797_M2 • ALG_DES_CBC_NOPAD • ALG_DES_ECB_ISO9797_M1 • ALG_DES_ECB_ISO9797_M2 • ALG_DES_ECB_NOPAD • ALG_DES_CBC_PKCS5 • ALG_DES_ECB_PKCS5
	[assignment: cryptographic key sizes]	LENGTH_DES3_2KEY, LENGTH_DES3_ 3KEY]
	[assignment: list of standards]	for ALG_DES_ECB_ISO9797_M2 see Java Card API Spec [23], for the rest see both [23] and JCOPX API [10]
FCS_COP.1.1 [AES]	[assignment: list of cryptographic operations]	decryption and encryption
	[assignment: cryptographic algorithm]	• ALG_AES_BLOCK_128_CBC_NOPAD • ALG_AES_BLOCK_128_CBC_NOPAD_ STANDARD • ALG_AES_BLOCK_128_ECB_NOPAD • ALG_AES_CBC_ISO9797_M2 • ALG_AES_CBC_ISO9797_M2_STANDARD • ALG_AES_ECB_ISO9797_M2 • ALG_AES_CBC_PKCS5 • ALG_AES_ECB_PKCS5
	[assignment: cryptographic key sizes]	LENGTH_AES_128, LENGTH_AES_192 and LENGTH_AES_256

SFR ID	Selection / Assignment text	Selection / Assignment value
	[assignment: list of standards]	for ALG_AES_BLOCK_128_CBC_NOPAD_see API specified in JCOPX [10], for the rest see Java Card API Spec [23]
FCS_COP.1.1 [RSACipher]	[assignment: list of cryptographic operations]	decryption and encryption
	[assignment: cryptographic algorithm]	• ALG_RSA_NOPAD • ALG_RSA_PKCS1 • ALG_RSA_PKCS1_OAEP
	[assignment: cryptographic key sizes]	any key length that is amultiple of 32 between 512 and 2048 bits
	[assignment: list of standards]	Java Card API Spec [23] and for the 32 bit step range see API specified in JCOPX [10]
FCS_COP.1.1 [ECDH_ P1363]	[assignment: list of cryptographic operations]	Diffie-Hellman Key Agreement
	[assignment: cryptographic algorithm]	• ALG_EC_SVDP_DH • ALG_EC_SVDP_DH_KDF • ALG_EC_SVDP_DH_PLAIN • ALG_EC_SVDP_DHC • ALG_EC_SVDP_DHC_KDF • ALG_EC_SVDP_DHC_PLAIN • ALG_EC_SVDP_DH_PLAIN_XY
	[assignment: cryptographic key sizes]	LENGTH_EC_FP_224,LENGTH_EC_FP_ 256,LENGTH_EC_FP_384,LENGTH_EC_FP_ 521 and from 224 bit to 528 bit in 1 bit steps]
	[assignment: list of standards]	Java Card API Spec [23] and for ALG_EC_SVDP_DH_PLAIN_or 1 bit step range key size see API specified in JCOPX [10]]
FCS_COP.1.1 [DESMAC]	[assignment: list of cryptographic operations]	MAC generation and verification
	[assignment: cryptographic algorithm]	Triple-DES in outer CBC for Mode: • ALG_DES_MAC4_ISO9797_1_M1_ALG3 • ALG_DES_MAC4_ISO9797_1_M2_ALG3 • ALG_DES_MAC4_ISO9797_M1 • ALG_DES_MAC4_ISO9797_M2 • ALG_DES_MAC8_ISO9797_1_M1_ALG3 • ALG_DES_MAC8_ISO9797_1_M2_ALG3 • ALG_DES_MAC8_ISO9797_M1 • ALG_DES_MAC8_ISO9797_M2 • ALG_DES_MAC8_NOPAD • ALG_DES_MAC4_PKCS5 • ALG_DES_MAC8_PKCS5
	[assignment: cryptographic key sizes]	LENGTH_DES3_2KEY, LENGTH_DES3_3KEY
	[assignment: list of standards]	Java Card API Spec [23] and JCOPX API [10]

SFR ID	Selection / Assignment text	Selection / Assignment value
FCS_COP.1.1 [RSASignature-PKCS1]	[assignment: list of cryptographic operations]	digital signature generation and verification
	[assignment: cryptographic algorithm]	• ALG_RSA_SHA_224_PKCS1 • ALG_RSA_SHA_224_PKCS1_PSS • ALG_RSA_SHA_256_PKCS1 • ALG_RSA_SHA_256_PKCS1_PSS • ALG_RSA_SHA_384_PKCS1 • ALG_RSA_SHA_384_PKCS1 • ALG_RSA_SHA_512_PKCS1 • ALG_RSA_SHA_512_PKCS1_PSS • SIG_CIPHER_RSA in combination with MessageDigest.ALG_SHA_256, MessageDigest.ALG_MessageDigest.ALG_SHA_512 and in combination with Cipher.PAD_PKCS1_OAEP
	[assignment: cryptographic key sizes]	any key length that is a multiple of 32 between 512 and 2048 bits
	[assignment: list of standards]	Java Card API Spec [23] and for the 32 bit step range see API specified in JCOPX [10]
FCS_COP.1.1 [ECSignature]	[assignment: list of cryptographic operations]	digital signature generation and verification
	[assignment: cryptographic algorithm]	• ALG_ECDSA_SHA_224 • ALG_ECDSA_SHA_256 • ALG_ECDSA_SHA_384 • ALG_ECDSA_SHA_512 • SIG_CIPHER_ECDSA in combination with MessageDigest.ALG_SHA_256 or MessageDigest.ALG_SHA_384 or MessageDigest.ALG_SHA_512
	[assignment: cryptographic key sizes]	LENGTH_EC_FP_128,LENGTH_EC_FP_160, LENGTH_EC_FP_192, LENGTH_EC_FP_224, LENGTH_EC_FP_256, LENGTH_EC_FP_384, LENGTH_EC_FP_521 and from 128 bit to 528 bit in 1 bit steps
	[assignment: list of standards]	Java Card API Spec [23] and for 1 bit step range key size see API specified in JCOPX [10]
FCS_COP.1.1 [SHA]	[assignment: list of cryptographic operations]	secure hash computation
	[assignment: cryptographic algorithm]	• ALG_SHA [1] • ALG_SHA_224 • ALG_SHA_256 • ALG_SHA_384 • ALG_SHA_512
	[assignment: cryptographic key sizes]	LENGTH_SHA,LENGTH_SHA_224, LENGTH_SHA_256, LENGTH_SHA_384, LENGTH_SHA_512
	[assignment: list of standards]	

SFR ID	Selection / Assignment text	Selection / Assignment value
FCS_COP.1.1 [AES_CMAC]	[assignment: list of cryptographic operations]	CMAC generation and verification
	[assignment: cryptographic algorithm]	• ALG_AES_CMAC16 • SIG_CIPHER_AES_CMAC16 • ALG_AES_CMAC16_STANDARD
	[assignment: cryptographic key sizes]	LENGTH_AES_128, LENGTH_AES_192 and LENGTH_AES_256 bit
	[assignment: list of standards]	assignment: see Java Card API Spec [23] and the JCOPX API specified in [10]
FCS_COP.1.1 [HMAC]	[assignment: list of cryptographic operations]	HMAC generation and verification
	[assignment: cryptographic algorithm]	• ALG_HMAC_SHA_256 • ALG_HMAC_SHA_384 • ALG_HMAC_SHA_512
	[assignment: cryptographic key sizes]	LENGTH_SHA_256,LENGTH_SHA_384 and LENGTH_SHA_512 bit
	[assignment: list of standards]	Java Card specification [23] and JCOPX API [10]
FCS_COP.1.1 [TDES_CMAC]	[assignment: list of cryptographic operations]	message authentication and verification
	[assignment: cryptographic algorithm]	• ALG_DES_CMAC8 • SIG_CIPHER_DES_CMAC8
	[assignment: cryptographic key sizes]	LENGTH_DES3_2KEY and LENGTH_DES3_3KEY bit
	[assignment: list of standards]	see API specified in JCOPX [10]
FCS_COP.1.1 [DAP]	[assignment: list of cryptographic operations]	verification of the DAP signature attached to Executable Load Applications
	[assignment: cryptographic algorithm]	• ALG_RSA_SHA_PKCS1 • ALG_ECDSA_SHA_256
	[assignment: cryptographic key sizes]	LENGTH_RSA_1024, LENGTH_EC_FP_256
	[assignment: list of standards]	GP Spec [33] and JCOPX API [10]

[1] Due to mathematical weakness only resistant against AVA_VAN.5 for temporary data (e.g. as used for generating session keys), but not if repeatedly applied to the same input data.

7.1.1.2.3 Card_security_management

The following table provides the assignments and/or selections of related SFRs taken from the JCOP PP [6]:

Table 58.

SFR ID	Selection / Assignment text	Selection / Assignment value
FAU_ARP.1.1	[assignment: list of other actions]	response with error code to S.CAD

SFR ID	Selection / Assignment text	Selection / Assignment value
FDP_SDI.2.1 [DATA]	[assignment: integrity errors]	integrity errors
	[assignment: user data attributes]	integrity protected data Application Note - The following data elements have the user data attribute ”integrity protected data”: • D.APP_KEYs • D.PIN • D.TOE_IDENTIFIER
FDP_SDI.2.2 [DATA]	[assignment: action to be taken]	reset the card session for integrity errors
FPR_UNO.1.1	[assignment: list of users and/ or subjects]	all users
	[assignment: list of operations]	all operations
	[assignment: list of objects]	D.APP_KEYs, D.PIN
	[assignment: list of protected users and/or subjects].	another user
FPT_TDC.1	[assignment: list of interpretation rules to be applied by the TSF]	none

7.1.1.2.4 AID Management

No assignments nor selections are needed for this group of SFRs defined the JCOP PP [6].

The following table provides the assignments and/or selections of related SFRs taken from the JCOP PP [6]:

Table 59.

SFR ID	Selection / Assignment text	Selection / Assignment value
FIA_USB.1.2/ AID	[assignment: rules for the initial association of attributes]	each uploaded package is associated with an unique Package AID
FIA_USB.1.3/ AID	[assignment: rules for the changing of attributes]	ehe initially assigned Package AID is unchangeable

7.1.1.3 INSTG Security Functional Requirements

The following table provides the assignments and/or selections of related SFRs taken from the JCOP PP [6]:

Note that the SFR FDP_ITC.2[INSTALLER] has been refined and is now part of the card management SFRs (FDP_ITC.2[CCM]).

Table 60.

SFR ID	Selection / Assignment text	Selection / Assignment value
FPT_RCV.3.1 [Installer]	[assignment: list of failures/ service discontinuities]	none
FPT_RCV.3.2 [Installer]	[assignment: list of failures/ service discontinuities]	a failure during load/installation of a package/ applet and deletion of a package/applet/object

SFR ID	Selection / Assignment text	Selection / Assignment value
FPT_RCV.3.3 [Installer]	[assignment: quantification]	0%

7.1.1.4 ADELG Security Functional Requirements

No assignments nor selections are needed for this group of SFRs defined the JCOP PP [6].

7.1.1.5 RMIG Security Functional Requirements

Not used in this ST because RMI is optional in PP [6] and the TOE does not support RMI.

7.1.1.6 ODELG Security Functional Requirements

No assignments nor selections are needed for this group of SFRs defined the JCOP PP [6].

7.1.1.7 CarG Security Functional Requirements

The card management SFRs from the PP [6] are refined by, replaced by and/or completed with the following SFRs.

FDP_UIT.1 [CCM] (refines FDP_UIT.1/ CM)	**Data exchange integrity (CCM)**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path].
FDP_UIT.1.1 [CCM]	The TSF shall enforce the **[assignment: Secure Channel Protocol information flow control policy and the Security Domain access control policy]** to **[selection:receive]** user data in a manner protected from **[selection:modification, deletion, insertion and replay]** errors.
FDP_UIT.1.2 [CCM]	The TSF shall be able to determine on receipt of user data, whether **[selection: modification, deletion, insertion, replay]** has occurred.

FDP_ROL.1 [CCM] (added)	**Basic rollback (CCM)**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_ROL.1.1 [CCM]	The TSF shall enforce **[assignment: Security Domain access control policy]** to permit the rollback of the **[assignment: installation operation]** on the **[assignment: executable files and application instances]**.
FDP_ROL.1.2 [CCM]	The TSF shall permit operations to be rolled back within the **[assignment: boundaries of available memory before the card content management function started]**.

FDP_ITC.2 [CCM] (replaces FDP_ITC.2/ INSTALLER)	**Import of user data with security attributes (CCM)**
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] [FTP_ITC.1 Inter-TSF trusted channel, or FTP_TRP.1 Trusted path] FPT_TDC.1 Inter-TSF basic TSF data consistency
FDP_ITC.2.1 [CCM]	The TSF shall enforce the **[assignment: Security Domain access control policy and the Secure Channel Protocol information flow policy]** when importing user data, controlled under the SFP, from outside of the TOE.
FDP_ITC.2.2 [CCM]	The TSF shall ignore any security attributes associated with the imported user data.
FDP_ITC.2.3 [CCM]	The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.
FDP_ITC.2.4 [CCM]	The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.
FDP_ITC.2.5 [CCM]	The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **[assignment:Package loading is allowed only if, for each dependent package, its AID attribute is equal to a resident package AID attribute, the major (minor) Version attribute associated to the dependent package is lesser than or equal to the major (minor) Version attribute associated to the resident package ([24], §4.5.2).]**.
Application Note	This SFR also covers security functionality required by Amendment A of the GP specification [27], i.e. personalizing SDs and loading ciphered load files.

FPT_FLS.1 [CCM]	**Failure with preservation of secure state (CCM)**
(added)	
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1 [CCM]	The TSF shall preserve a secure state when the following types of failures occur: **[assignment: the Security Domain fails to load/install an Executable File/application instance as described in [25], Section 11.1.5]**.

FDP_ACC.1 [SD]	**Subset access control (SD)**
(added)	
Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control.
FDP_ACC.1.1 [SD]	The TSF shall enforce the **[assignment: Security Domain access control policy]** on **[assignment:** • Subjects: S.INSTALLER, S.ADEL, S.CAD (from [6]) and S.SD • Objects: Delegation Token, DAP Block and Load File • Operations: GlobalPlatform's card content management APDU commands and API methods **]**.

FDP_ACF.1 [SD]	**Security attribute based access control (SD)**
(added)	
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1 [SD]	The TSF shall enforce the **[assignment: Security Domain access control policy]** to objects based on the following **[assignment:** • **Subjects:** – **S.INSTALLER, defined in [6] and represented by the GlobalPlatform Environment (OPEN) on the card, the Card Life Cycle attributes (defined in Section 5.1.1 of [26])** – **S.ADEL, also defined in [6] and represented by the GlobalPlatform Environment (OPEN) on the card**

– S.SD receiving the Card Content Management commands (through APDUs or APIs) with a set of Privileges (defined in Section 6.6.1 of [26]), a Life-cycle Status (defined in Section 5.3.2 of [26]) and a Secure Communication Security Level (defined in Section 10.6 of [26])

– S.CAD, defined in [6], the off-card entity that communicates with the S.INSTALLER and S.ADEL through S.SD

- **Objects:**
  - **The Delegation Token, in case of Delegated Management operations, with the attributes Present or Not Present**
  - **The DAP Block, in case of application loading, with the attributes Present or Not Present**
  - **The Load File or Executable File, in case of application loading, installation, extradition or registry update, with a set of intended privileges and its targeted associated SD AID.**
- **Mapping subjects/objects to security attributes:**
  - **S.INSTALLER: Security Level, Card Life Cycle, Life-cycle Status, Privileges, Resident Packages, Registered Applets**
  - **S.ADEL: Active Applets, Static References, Card Life Cycle, Life-cycle Status, Privileges, Applet Selection Status, Security Level**
  - **S.SD: Privileges, Life-cycle Status, Security Level**
  - **S.CAD: Security Level**

]

FDP_ACF.1.2 [SD]	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[assignment: Runtime behavior rules defined by GlobalPlatform for:** • **loading (Section 9.3.5 of [26])** • **installation (Section 9.3.6 of [26])** • **extradition (Section 9.4.1 of [26])** • **registry update (Section 9.4.2 of [26])** • **content removal (Section 9.5 of [26])** **]**
FDP_ACF.1.3 [SD]	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: none]**
FDP_ACF.1.4 [SD]	The TSF shall explicitly deny access of subjects to objects based on the following additional rules:**[assignment: when at least one of the rules defined by GlobalPlatform does not hold]**
Application Note	FDP_ACF.1.2 [SD]

- This policy introduces the notion of reachability, which provides a general means to describe objects that are referenced from a certain applet instance or package.
- S.ADEL calls the ”uninstall” method of the applet instance to be deleted, if implemented by the applet, to inform it of the deletion request. The order in which these calls and the dependencies checks are performed are out of the scope of this protection profile.

FMT_MSA.1 [SD]	**Management of security attributes (SD)**
(added)	
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1 [SD]	The TSF shall enforce the **[assignment: Security Domain access control policy]** to restrict the ability to **[selection: modify]** the security attributes **[assignment:** • **Card Life Cycle,** • **Privileges,** • **Life-cycle Status,** • **Security Level.** **]** to **[assignment: the Security Domain and the application instance itself]**.

FMT_MSA.3 [SD]	**Static attribute initialisation (SD)**
(added)	
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1 [SD]	The TSF shall enforce the **[assignment: Security Domain access control policy]** to provide **[restrictive]** default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 [SD]	The TSF shall allow the **[assignment: Card Issuer or the Application Provider]** to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1 [SD]	**Specification of Management Functions (SD)**

(refines FMT_SMF.1/CM)

Hierarchical to: No other components.

Dependencies: No dependencies.

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

- **Management functions specified in GlobalPlatform specifications [GP]:**
  - **card locking (Section 9.6.3 of [26])**
  - **application locking and unlocking (Section 9.6.2 of [26])**
  - **card termination (Section 9.6.4 of [26])**
  - **card status interrogation (Section 9.6.6 of [26])**
  - **application status interrogation (Section 9.6.5 of [26])**

].

FMT_SMR.1 [SD] Security roles (SD)

(refines FMT_SMR.1/CM)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 [SD] The TSF shall maintain the roles **[assignment: ISD, SSD]**.

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

FCO_NRO.2 [SC] Enforced proof of origin (SC)

(refines FCO_NRO.2/CM)

Hierarchical to: FCO_NRO.1 Selective proof of origin.

Dependencies: FIA_UID.1 Timing of identification.

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

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

FCO_NRO.2.3 [SC] The TSF shall provide a capability to verify the evidence of origin of information to **[selection: originator]** given **[assignment:**

at the time the Executable load files are received as no evidence is kept on the card for future verification].

Application Note

FCO_NRO.2.1[

[SC]

- 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[SC]:

- 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.

FDP_IFC.2 [SC] (refines FDP_IFC.2/CM)	**Complete information flow control (SC)**
Hierarchical to:	FDP_IFC.1 Subset information flow control.
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.2.1 [SC]	The TSF shall enforce the **[assignment: Secure Channel Protocol information flow control policy]** on **[assignment:** • **the subjects S.CAD and S.SD, involved in the exchange of messages between the TOE and the CAD through a potentially unsafe communication channel,** • **the information controlled by this policy are the card content management commands, including personalization commands, in the APDUs sent to the card and their associated responses returned to the CAD** • **[assignment: none]** **]** and all operations that cause that information to flow to and from subjects covered by the SFP.
FDP_IFC.2.2 [SC]	The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.
FDP_IFF.1 [SC] (refines FDP_IFF.1/CM)	**Simple security attributes (SC)**

Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1.1 [SC]	The TSF shall enforce the **[assignment: Secure Channel Protocol information flow control policy]** based on the following types of subject and information security attributes **[assignment: :** • **Subjects:** – **S.SD receiving the Card Content Management commands (through APDUs or APIs).** – **S.CAD the off-card entity that communicates with the S.SD.** • **Information:** – **executable load file, in case of application loading;** – **applications or SD privileges, in case of application installation or registry update;** – **personalization keys and/or certificates, in case of application or SD personalization.** • **[assignment: none]** **]**
FDP_IFF.1.2 [SC]	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[assignment:** • **Runtime behavior rules defined by GlobalPlatform for:** – **loading (Section 9.3.5 of [26]);** – **installation (Section 9.3.6 of [26]);** – **extradition (Section 9.4.1 of [26]);** – **registry update (Section 9.4.2 of [26]);** – **content removal (Section 9.5 of [26])** **]**
FDP_IFF.1.3 [SC]	The TSF shall enforce the **[assignment: none]**
FDP_IFF.1.4 [SC]	The TSF shall explicitly authorise an information flow based on the following rules: **[assignment:none]**
FDP_IFF.1.5 [SC]	The TSF shall explicitly deny an information flow based on the following rules: **[assignment:]** • When none of the conditions listed in the element FDP_IFF.1.4 of this component hold and at least one of those listed in the element FDP_IFF.1.2 does not hold **]**.

Application note	The subject S.SD can be the ISD or APSD.
Application note	The on-card and the off-card subjects have security attributes such as MAC, Cryptogram, Challenge, Key Set, Static Keys, etc.

FMT_MSA.1 [SC] **Management of security attributes (SC)**

(refines FMT_MSA.1/CM)

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1 [SC]	The TSF shall enforce the **[assignment: SSecure Channel Protocol information flow control policy]** to restrict the ability to **[selection: modify]** the security attributes **[assignment:** • **Key Set,** • **Security Level,** • **Secure Channel Protocol,** • **Session Keys,** • **Sequence Counter,** • **ICV.** **]** to **[assignment: the actor associated with the according security domain:** • **The Card Issuer for ISD,** • **The Application Provider for APSD** **]**.
Application note	The key data used for setting up a secure channel is according to GP spec [26], Amendment D [32] and Amendmend F [34].

FMT_MSA.3 [SC] **Static attribute initialisation (SC)**

(refines FMT_MSA.3/CM)

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1 [SC]	The TSF shall enforce the **[assignment: Secure Channel Protocol information flow control policy]** to provide

	[restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 [SC]	The TSF shall allow the **[assignment: Card Issuer, Application Provider]** to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1 [SC] (refines FMT_SMF.1/CM)	**Specification of Management Functions (SC)**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1 [SC]	The TSF shall be capable of performing the following management functions: **[assignment:** • **Management functions specified in GlobalPlatform specifications [GP]:** **– loading (Section 9.3.5 of [26])** **– installation (Section 9.3.6 of [26])** **– extradition (Section 9.4.1 of [26])** **– registry update (Section 9.4.2 of [26])** **– content removal (Section 9.5 of [26])** **]**.
Application note	All management functions related to secure channel protocols shall be relevant.

FIA_UID.1 [SC] (refines FIA_UID.1/CM)	**Timing of Identification (SC)**
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1 [SC]	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 [SC]	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Application Note	The GlobalPlatform TSF mediated actions listed in [GP] such as selecting an application, requesting data, initializing, etc.

FIA_UAU.1 [SC]	**Timing of authentication (SC)**
(added)	
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
FIA_UAU.1.1 [SC]	The TSF shall allow **[assignment: the TSF mediated actions listed in FIA_UID.1[SC]]** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2 [SC]	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.4 [SC]	**Single-use authentication mechanisms (SC)**
(added)	
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.4.1 [SC]	The TSF shall prevent reuse of authentication data related to **[assignment: the authentication mechanism used to open a secure communication channel with the card]**

FTP_ITC.1 [SC]	**Inter-TSF trusted channel(SC)**
(refines FTP_ITC.1/ CM)	
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FTP_ITC.1.1 [SC]	The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 [SC]	The TSF shall permit **[selection: another trusted IT product]** to initiate communication via the trusted channel.
FTP_ITC.1.3 [SC]	The TSF shall initiate communication via the trusted channel for **[assignment: all card management functions including:** • **loading;** • **installation;** • **extradition;** • **registry update;** • **content removal;** • **changing the Application Life Cycle or Card Life Cycle;** • **SD personalization.** **]**.

7.1.1.8 EMG Security Functional Requirements

Not used in this ST because EMG is optional in PP [6] and the TOE does not support EMG.

7.1.1.9 Further Security Functional Requirements

The SFRs in this section provide JCOP additional proprietary features related SFRs.

FAU_SAS.1 [SCP]	**Audit Data Storage (SCP)**
(added)	
Hierarchical to:	No other components.
Dependencies:	No other components.
FAU_SAS.1.1 [SCP]	The TSF shall provide **[assignment: test personnel before TOE Delivery]** with the capability to store the **[assignment: Initialisation Data and/or Prepersonalisation Data and/or supplements of the Smartcard Embedded Software]** in the **[assignment: audit records]**.

FCS_RNG.1	**Random Number Generation.**
(added)	
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RNG.1.1	The TSF shall provide a **[selection: hybrid deterministic]** random number generator that implements: **[assignment:** • **(DRG.3.1) If initialized with a random seed using a PTRNG of class PTG.2 (as defined in [46]) as random source, the**

	internal state of the RNG shall have at least 256 bit of entropy. • **(DRG.3.2) The RNG provides forward secrecy (as defined in [46]).** • **(DRG.3.3) The RNG provides enhanced backward secrecy even if the current internal state is known (as defined in [46])** **]**.
FCS_RNG.1.2	The TSF shall provide **[selection: random numbers]** that meet **[assignment: a defined quality metric]** • **(DRG.3.4) The RNG, initialized with a random seed using a PTRNG of class PTG.2 (as defined in [46]) as random source, generates output for which for AES-mode 248 and for TDEA-mode 235 strings of bit length 128 are mutually different with probability at least 1-2^24** • **(DRG.3.5) Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A (as defined in [46]).** **]**.
Application Note	This functionality is provided by the certified Security Software, see [22]

FIA_AFL.1 [PIN]	**Basic Authentication Failure Handling (PIN)**
(added)	
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FIA_AFL.1.1 [PIN]	The TSF shall detect when **[selection: an administrator configurable positive integer within [1 and 127]]** unsuccessful authentication attempts occur related to **[assignment: any user authentication using D.PIN]**.
FIA_AFL.1.2 [PIN]	When the defined number of unsuccessful authentication attempts has been **[selection: surpassed]**, the TSF shall **[assignment: block the authentication with D.PIN]**.
Application Note	The dependency with FIA_UAU.1 is not applicable. The TOE implements the firewall access control SFP, based on which access to the object implementing FIA_AFL.1[PIN] is organized.

FPT_EMSEC.1	**TOE Emanation**
(added)	

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_EMSEC.1.1	The TOE shall ensure **[assignment: variations in power consumption or timing during command execution]** is unable to use the following interface **[assignment: non-useful information]** to gain access to **[assignment: TSF data: D.CRYPTO]** and **[assignment: User data: D.PIN, D.APP_KEYs]**.
FPT_EMSEC.1.2	The TOE shall ensure **[assignment: that unauthorized users]** is unable to use the following interface **[assignment: electrical contacts or RF field]** to gain access to **[assignment: TSF data D.CRYPTO]** and **[assignment: User data D.PIN, D.APP_KEYS]**.

FPT_PHP.3	**Resistance to physical attack**
(added)	
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.3.1	The TSF shall resist **[assignment: physical manipulation and physical probing]** to the **[assignment: TSF]** by responding automatically such that the SFRs are always enforced.
Refinement	The TSF will implement appropriate mechanisms to continuously counter physical manipulation and physical probing. Due to the nature of these attacks (especially manipulation) the TSF can by no means detect attacks on all of its elements. Therefore, permanent protection against these attacks is required ensuring that security functional requirements are enforced. Hence, ”automatic response” means here (i) assuming that there might be an attack at any time and (ii) countermeasures are provided at any time.
Application Note	This SFR is taken from the certified Security IC Platform Protection Profile [5].

7.1.1.10 Configuration Security Functional Requirements

FDP_IFC.2 [CFG]	**Complete information flow control (CFG)**
(added)	
Hierarchical to:	FDP_IFC.1 Subset information flow control.

Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.2.1 [CFG]	The TSF shall enforce the **[assignment: CONFIGURATION information flow control SFP]** on **[assignment: S.Customer, S.NXP, S.ConfigurationMechanism, and D.CONFIG_ITEM]**.
FDP_IFC.2.2 [CFG]	The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

FDP_IFF.1 [CFG] **Simple security attributes**

(added)

Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1.1 [CFG]	The TSF shall enforce the **[assignment: CONFIGURATION information flow control SFP]** based on the following types of subject and information security attributes **[assignment:** • **S.Customer: security attributes Customer Configuration Token** • **S.NXP: security attributes NXP Configuration Token generation key** • **S.ConfigurationMechanism: security attributes NXP Configuration Access, Customer Configuration Access** • **D.CONFIG_ITEM: security attributes access privilege** **]**.
FDP_IFF.1.2 [CFG]	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[assignment:** • **Read and write operations of D.CONFIG_ITEM between S.ConfigurationMechanism and S.NXP shall only be possible when S.NXP is authenticated with its token using the NXP Configuration Token generation key.** • **Read and write operations of D.CONFIG_ITEM between S.ConfigurationMechanism and S.Customer shall only be possible when S.Customer is authenticated with its token using the Customer Configuration Token and if access privilege allows it.** • **Enabling or disabling of NXP Configuration Access between S.ConfigurationMechanism and S.NXP shall only be possible when S.NXP is authenticated with its token using the NXP Configuration Token generation key.** **]**.

FDP_IFF.1.3 [CFG]	The TSF shall enforce the additional information flow control SFP rules **[assignment: none]**
FDP_IFF.1.4 [CFG]	The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: none]**
FDP_IFF.1.5 [CFG]	The TSF shall explicitly deny an information flow based on the following rules: **[assignment:** • **If the NXP Configuration Access is disabled then nobody can read or write D.CONFIG_ITEM.** • **If the Customer Configuration Access is disabled then S.Customer can not read or write D.CONFIG_ITEM.** **]**.
Application note	GlobalPlatform Framework authentication mechnism is used to authenticate the tokens.

FIA_UID.1 [CFG]	**Timing of Identification (CFG)**
(added)	
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1 [CFG]	The TSF shall allow **[assignment: to select the configuration applet]** on behalf of the user to be performed before the user is identified
FIA_UID.1.2 [CFG]	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FMT_MSA.1 [CFG]	**Management of security attributes (CFG)**
(added)	
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1 [CFG]	The TSF shall enforce the **[assignment: CONFIGURATION information flow control SFP]** to restrict the ability to **[selection: modify]** the security attributes **[assignment: NXP Configuration Access and Customer Configuration Access]** to **[assignment: S.NXP and S.Customer]**.

FMT_MSA.3 [CFG]	**Static attribute initialisation (CFG)**
(added)	
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1 [CFG]	The TSF shall enforce the **[assignment: CONFIGURATION information flow control SFP]** to provide **[restrictive]** default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 [CFG]	The TSF shall allow the **[assignment: nobody]** to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1 [CFG]	**Specification of Management Functions (CFG)**
(added)	
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1 [CFG]	The TSF shall be capable of performing the following management functions: **[assignment: disable the NXP Configuration Access, disable the Customer Configuration Access]**

FMT_SMR.1 [CFG]	**Security roles (CFG)**
(added)	
Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1 [CFG]	The TSF shall maintain the roles **[assignment: S.NXP and S.Customer]**.
FMT_SMR.1.2 [CFG]	The TSF shall be able to associate users with roles.
Application note	The roles of the CONFIGURATION information flow control SFP are defined by the NXP Configuration Token generation key and the Customer Configuration Token.

7.1.1.11 OS update Security Functional Requirements

The SFRs in this section provide JCOP OS Update proprietary features related SFRs.

FDP_IFC.2 [OSU]	**Complete information flow control (OSU)**
(added)	
Hierarchical to:	FDP_IFC.1 Subset information flow control.
Dependencies:	FDP_IFF.1 Simple security attributes
FDP_IFC.2.1 [OSU]	The TSF shall enforce the **[assignment: OS Update information flow control SFP]** on **[assignment: S.OSU and D.UPDATE_IMAGE]**.
FDP_IFC.2.2 [OSU]	The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

FDP_IFF.1 [OSU]	**Simple security attributes**
(added)	
Hierarchical to:	No other components.
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
FDP_IFF.1.1 [OSU]	The TSF shall enforce the **[assignment: OS Update information flow control SFP]** based on the following types of subject and information security attributes **[assignment:** • **S.OSU: security attributes Current Sequence Number, Verification Key, Package Decryption Key** • **D.UPDATE_IMAGE: security attributes Received Sequence Number, Image Type** **]**.
FDP_IFF.1.2[OSU]	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[assignment:** • **S.OSU shall only accept D.UPDATE_IMAGE which signature can be verified with Verification Key.** • **S.OSU shall only accept D.UPDATE_IMAGE for the update process that can be decrypted with Package Decryption Key.** **]**.

FDP_IFF.1.3 [OSU]	The TSF shall enforce the additional information flow control SFP rules **[assignment: S.OSU shall only authorize D.UPDATE_IMAGE for the update process if the following rules apply:** • **If Image Type equals Reset then Received Sequence Number shall equal Current Sequence Number.** • **If Image Type equals Upgrade then Received Sequence Number shall be higher than Current Sequence Number.** • **If Image Type equals Downgrade then Received Sequence Number shall be lower than Current Sequence Number.** **]**.
FDP_IFF.1.4 [OSU]	The TSF shall explicitly authorise an information flow based on the following rules: **[assignment: none]**
FDP_IFF.1.5[OSU]	The TSF shall explicitly deny an information flow based on the following rules: **[assignment: D.Update_image which is not included in the pre-loaded OS Update plan]**
Application note	The on-card S.OSU role interacts with the off-card S.UpdateImageCreator via OSU commands. The D.UPDATE_IMAGE is split up into smaller chunks and transmitted as payload within the OSU Commands to the TOE.
Application note	Decrypting the D.UPDATE_IMAGE with the Package Decryption Key prevents the authorization of the D.UPDATE_IMAGE for the update process on a not certified system. The Package Decryption Key is only available on a certified TOE.

FMT_MSA.3 [OSU]	**Static attribute initialisation (OSU)**
(added)	
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1 [OSU]	The TSF shall enforce the **[assignment: OS Update information flow control SFP]** to provide **[restrictive]** default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 [OSU]	The TSF shall allow the **[assignment: S.OSU]** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.1 [OSU]	**Management of security attributes (OSU)**

(added)

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1 [OSU]	The TSF shall enforce the **[assignment: OS Update information flow control SFP]** to restrict the ability to **[selection: modify]** the security attributes **[assignment: Current Sequence Number]** to **[assignment: S.OSU]**.

FMT_SMR.1 [OSU] Security roles (OSU)

(added)

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification
FMT_SMR.1.1 [OSU]	The TSF shall maintain the roles **[assignment: S.OSU]**.
FMT_SMR.1.2 [OSU]	The TSF shall be able to associate users with roles.

FMT_SMF.1 [OSU] Specification of Management Functions (OSU)

(added)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1 [OSU]	The TSF shall be capable of performing the following management functions: **[assignment:** • **query Current Sequence Number** • **query Reference Sequence Number** **]**.
Application note	After the atomic activation of the additional code the Final Sequence Number is returned on querying the Current Sequence Number.

FIA_UID.1 [OSU] Timing of Identification (OSU)

(added)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1 [OSU]	The TSF shall allow **[assignment: OP.TRIGGER_UPDATE]** on behalf of the user to be performed before the user is identified
FIA_UID.1.2 [OSU]	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.1 [OSU] **Timing of authentication (OSU)**

(added)

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
FIA_UAU.1.1 [OSU]	The TSF shall allow **[assignment: OP.TRIGGER_UPDATE]** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2 [OSU]	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UAU.4 [OSU] **Single-use authentication mechanisms (OSU)**

(added)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UAU.4.1[OSU]	The TSF shall prevent reuse of authentication data related to **[assignment: the authentication mechanism used to load D.UPDATE_IMAGE]**

FPT_FLS.1 [OSU] **Failure with preservation of secure state (OSU)**

(added)

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_FLS.1.1 [OSU]	The TSF shall preserve a secure state when the following types of failures occur: **[assignment:**

- **Corrupted D.UPDATE_IMAGE is received.**
- **Unauthorized D.UPDATE_IMAGE is received.**
- **The OS Update Process is interrupted.**
- **The activation of the additional code failed.**

].

7.1.1.12 Restricted Mode Security Functional Requirements

The SFRs in this section provide JCOP Restricted Mode proprietary features related SFRs.

FDP_ACC.2 [RM]	**Complete access control (RM)**
(added)	
Hierarchical to:	FDP_ACC.1 Subset access control
Dependencies:	FDP_ACF.1 Security attribute based access control
FDP_ACC.2.1 [RM]	The TSF shall enforce the **[assignment: Restricted Mode access control SFP]** on **[assignment: S.SD, S.ACAdmin]** and all operations among subjects and objects covered by the SFP.
FDP_ACC.2.2 [RM]	The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

FDP_ACF.1 [RM]	**Security attribute based access control (RM)**
(added)	
Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
FDP_ACF.1.1 [RM]	The TSF shall enforce the **[assignment: Restricted Mode access control SFP]** to objects based on the following **[assignment:** • **S.SD: security attributes D.ATTACK_COUNTER** • **S.ACAdmin: security attributes D.ATTACK_COUNTER** **]**
FDP_ACF.1.2 [RM]	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[assignment:The D.ATTACK_COUNTER can be reset by S.ACAdmin or by the ISD]**

FDP_ACF.1.3 [RM]	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[assignment: none]**.
FDP_ACF.1.4 [RM]	The TSF shall explicitly deny access of subjects to objects based on the following additional rules:**[assignment: Deny all operations on all objects if the D.ATTACK_COUNTER has reached its limit (restricted mode), except for operations listed in FMT_SMF.1[RM]]**.
Application Note	FDP_ACF.1.2[RM]: • This policy introduces the notion of reachability, which provides a general means to describe objects that are referenced from a certain applet instance or package. • S.RM calls the ”uninstall” method of the applet instance to be deleted, if implemented by the applet, to inform it of the deletion request. The order in which these calls and the dependencies checks are performed are out of the scope of this protection profile.

FMT_MSA.3 [RM]	**Static attribute initialisation (RM)**
(added)	
Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1 [RM]	The TSF shall enforce the **[assignment: Restricted Mode access control SFP]** to provide **[restrictive]** default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2 [RM]	The TSF shall allow the **[assignment: nobody]** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.1 [RM]	**Management of security attributes (RM)**
(added)	
Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control], FMT_SMR.1 Security roles, FMT_SMF.1 Specification of Management Functions
FMT_MSA.1.1 [RM]	The TSF shall enforce the **[assignment: Restricted Mode access control]** to restrict the ability to **[selection: modify]** the

	security attributes **[assignment: D.ATTACK_COUNTER]** to **[assignment: ISD, S.ACAdmin]**.

FMT_SMF.1 [RM]	**Specification of Management Functions (RM)**
(added)	
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FMT_SMF.1.1 [RM]	The TSF shall be capable of performing the following management functions: **[assignment:** • **reset D.ATTACK_COUNTER.** • **select ISD.** • **authentication against the ISD.** • **initialize a Secure Channel with the card.** • **query the Serial Number (Unique ID for chip).** • **read Platform Identifier.** • **query the logging information.** • **read Secure Channel Sequence Counter.** • **read Current Sequence Number.** **]**.
Application note	After the atomic activation of the additional code the Final Sequence Number is returned on querying the Current Sequence Number.

FIA_UID.1 [RM]	**Timing of Identification (RM)**
(added)	
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FIA_UID.1.1 [RM]	The TSF shall allow **[assignment:** • **authenticate to ISD** • **identify the card** • **query the debug logging information** • **send Restricted Mode Unlock Request** • **read some of the sensitive data (see [10], section 4.1)** • **store some of the sensitive data in eUICC domain (see [10], section 4.1)** **]** on behalf of the user to be performed before the user is identified

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

FIA_UAU.1 [RM] **Timing of authentication (RM)**

(added)

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
FIA_UAU.1.1 [RM]	The TSF shall allow **[assignment:** • **authenticate to ISD** • **identify the card** • **query the debug logging information** • **send Restricted Mode Unlock Request** • **read some of the sensitive data (see [10], section 4.1)** • **store some of the sensitive data in eUICC domain (see [10], section 4.1)** **]** on behalf of the user to be performed before the user is authenticated.
FIA_UAU.1.2 [RM]	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

7.1.2 eUICC

The Security Functional Requirements for the eUICC component of the TOE are defined in strict compliance with the Security Problem Definition described in the eUICC PP [7].

The following table provides the selection and assignments for SFRs:

Table 61.

SFR ID	Selection / Assignment text	Selection / Assignment value
FIA_UID.1.1 [EXT]	[assignment: list of additional TSF mediated actions]	no additional TSF mediated actions
FIA_UAU.1.1 [EXT]	[assignment: list of additional TSF mediated actions]	no additional TSF mediated actions
FIA_UID.1.1 [MNO-SD]	[assignment: list of TSF-mediated actions]	• application selection • requesting data that identifies the eUICC
FDP_IFF.1.3 [SCP]	[assignment: additional information flow control SFP rules]	no additional information flow control SFP rules

SFR ID	Selection / Assignment text	Selection / Assignment value
FDP_IFF.1.4 [SCP]	[assignment: rules, based on security attributes, that explicitly authorise information flows]	none
FTP_ITC.1.3 [SCP]	[assignment: list of functions for which a trusted channel is required]	The TSF shall permit the SM-DP+ to open a SCP-SGP22 secure channel to transmit the following operations: • ES8+.InitialiseSecureChannel • ES8+.ConfigureISDP • ES8+.StoreMetadata • ES8+.ReplaceSessionKeys • ES8+.LoadProfileElements The TSF shall permit the remote OTA Platform to open a SCP80 or SCP81 secure channel to transmit the following operation: ES6.UpdateMetadata.
FDP_ITC.2.5 [SCP]	[assignment: additional importation control rules]	none
FPT_TDC.1.2 [SCP]	[assignment: list of interpretation rules to be applied by the TSF]	the rules defined in GSMA SGP.22 Specification [38], [39]
FCS_CKM.2 [SCP-MNO]	[assignment: cryptographic key distribution method]	set keys and components of DES, AES, RSA, RSA-CRT, EC, secure messaging and Network Authentication Algorithms EC
	[assignment: list of standards]	[23], [10], [11]
FCS_CKM.4.1 [SCP-SCM]	[assignment: cryptographic key destruction method]	physically overwriting the keys in a randomized manner
	[assignment: list of standards]	none
FCS_CKM.4.1 [SCP-MNO]	[assignment: cryptographic key destruction method]	physically overwriting the keys in a randomized manner
	[assignment: list of standards]	none
FDP_ACF.1.3 [ISDR]	[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]	ISDR shall perform the following operations: • ES8+.ConfigureISDP (Create and configure profile) • ES8+.StoreMetadata (Store profile metadata) • ES10c.EnableProfile (Enable profile) • ES10c.DisableProfile (Disable profile) • ES10c.DeleteProfile (Delete profile) • ES10c.eUICCMemoryReset (Perform a Memory reset) based on Profile ”state” and profile policy rules ”PPR”
FDP_ACF.1.4 [ISDR]	[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]	when any of the defined rules by SGP.22 Specification [38], [39], related to Profile ”state” and profile policy rules ”PPR” do not hold

SFR ID	Selection / Assignment text	Selection / Assignment value
FDP_ACC.1.1 [ECASD]	[assignment: additional list of subjects, objects, and operations between subjects and objects covered by the SFP]	• additional operations defined by the interfaces ES8+ (SM-DP+ – eUICC), and ES10x (LPA – eUICC) • creation of an eUICC signature on material provided by an ISD-R
FDP_ACF.1.1 [ECASD]	[assignment: additional list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]	none
FDP_ACF.1.2 [ECASD]	[assignment: additional rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]	Rules defined in section 2.4.of GSMA SGP.22 Specification [38], [39]
FDP_ACF.1.3 [ECASD]	[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]	none
FDP_ACF.1.4 [ECASD]	[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]	none
FDP_IFF.1.3 [Platform-Services]	[assignment: additional information flow control SFP rules]	no additional information flow control SFP rules
FDP_IFF.1.4 [Platform-Services]	[assignment: rules, based on security attributes, that explicitly authorise information flows]	none
FDP_IFF.1.5 [Platform-Services]	[assignment: rules, based on security attributes, that explicitly deny information flows]	• when none of the conditions listed in the element FDP_IFF.1.4 of this component. • Hold and at least one of those listed in the element FDP_IFF.1.2 does not hold.
FPT_FLS.1.1 [Platform-Services]	[assignment: other type of failure]	none
FPT_EMSEC.1.1 [eUICC]	[assignment: types of emissions]	variations in power consumption or timing during command execution
	[assignment: specified limits]	non-useful information
FPT_EMSEC.1.2 [eUICC]	[assignment: type of users]	that unauthorized users
	[assignment: type of connection]	electrical contacts or RF field
FMT_SMF.1 [eUICC]	[assignment: list of management functions to be provided by the TSF]	Profile Management functions specified in GSMA SGP.22 [38], [39]

SFR ID	Selection / Assignment text	Selection / Assignment value
FCS_CKM.2.1 [Mobile_ network]	[assignment: cryptographic key distribution method]	set keys and components of DES, AES, RSA, RSA-CRT, EC, secure messaging and Network Authentication Algorithms EC
	[assignment: list of standards]	[23], [10], [11]
FCS_COP.1.1 [Mobile_ network]	[selection: other algorithm, no other algorithm]	other algorithms (USIM_TEST and CDMA)
FCS_CKM.4.1 [Mobile_ network]	[assignment: cryptographic key destruction method]	physically overwriting the keys in a randomized manner
	[assignment: list of standards]	none

7.1.3 CSP

The Security Functional Requirements for the CSP component of the TOE are defined in strict compliance with the Security Problem Definition described in the CSP PP [8].

The following table provides the selection and assignments for SFRs:

Table 62.

SFR ID	Selection / Assignment text	Selection / Assignment value
FDP_ACC.1.1 [KM]	(1) [selection: Administrator, Crypto-Officer]	Administrator
FMT_MSA.1.1 [KM]	(1) [selection: Administrator, Crypto-Officer] (4) [selection: Administrator, Crypto-Officer] (5) [selection: Administrator, Crypto-Officer, Key Owner]	Administrator Administrator Administrator, Key Owner
FMT_MSA.3.2 [KM]	[selection: Administrator, Crypto-Officer]	Administrator
FMT_MTD.1.1 [KM]	(1) [selection: Administrator, Crypto-Officer, Key Owner]] (2) [selection: Administrator, Crypto-Officer] (3) [selection: Administrator, Crypto-Officer, Key Owner] (4) [selection: Administrator, Crypto-Officer, Key Owner]	Administrator, Key Owner Administrator Administrator, Key Owner Administrator, Key Owner
FMT_MTD.1.1 [RK]	(1) [selection: Administrator, Crypto-Officer] (2) [selection: Administrator, Crypto-Officer]	Administrator Administrator
FCS_CKM.1.1 [AES]	[selection: 256 bits, no other key size]	256 bits
FCS_CKM.5.1 [AES]	[assignment: input parameters]	derivation data
	[selection: 256 bits, no other key size]	256 bits

SFR ID	Selection / Assignment text	Selection / Assignment value
FCS_CKM.1.1 [ECC]	[selection: elliptic curves in the table 2 ([8])]	• brainpoolP256r1 • brainpoolP384r1 • brainpoolP521r1 • Curve P-256 • Curve P-384 • Curve P-521
	[selection: key size in the table 2 ([8])]	• 256-bit • 384-bit • 521-bit • 256-bit • 384-bit • 521-bit
	[selection: standards in the table 2 ([8])]	• RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111] • RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111] • RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111] • FIPS PUB 186-4 B.4 and D.1.2.3 [FIPS PUB 186-4] • FIPS PUB 186-4 B.4 and D.1.2.4 [FIPS PUB 186-4] • FIPS PUB 186-4 B.4 and D.1.2.5 [FIPS PUB 186-4]
FCS_CKM.5.1 [ECC]	[assignment: input parameters]	derivation data
	[selection: elliptic curves in table 2 ([8])]	• brainpoolP256r1 • brainpoolP384r1 • brainpoolP521r1 • Curve P-256 • Curve P-384 • Curve P-521
	[assignment: KDF]	CSP KDF
	[selection: key size in the table 2 ([8])]	• 256-bit • 384-bit • 521-bit • 256-bit • 384-bit • 521-bit

SFR ID	Selection / Assignment text	Selection / Assignment value
	[selection: standards in the table 2 ([8])]	• RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111] • RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111] • RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111] • FIPS PUB 186-4 B.4 and D.1.2.3 [FIPS PUB 186-4] • FIPS PUB 186-4 B.4 and D.1.2.4 [FIPS PUB 186-4] • FIPS PUB 186-4 B.4 and D.1.2.5 [FIPS PUB 186-4]
FCS_CKM.1.1 [RSA]	[assignment: cryptographic key sizes]	from 2000 bit, up to 4096 bit in 8 bit steps
FCS_CKM.5.1 [ECDHE]	[selection: AES-256, none other]	AES-256
	[selection: elliptic curves in table 2 ([8])]	• brainpoolP256r1 • brainpoolP384r1 • brainpoolP521r1 • Curve P-256 • Curve P-384 • Curve P-521
	[selection: DH group in table 3 ([8])]	• 256-bit random ECP group • 384-bit random ECP group • 521-bit random ECP group • brainpoolP256r1 • brainpoolP384r1 • brainpoolP521r1
	[assignment: key derivation function]	ANSI X9.63 key derivation function
	[selection:256 bits, none other]	256-bit
FCS_CKM.1.1 [ECKA-EG]	[selection: elliptic curves in table 2 ([8])]	• brainpoolP256r1 • brainpoolP384r1 • brainpoolP521r1 • Curve P-256 • Curve P-384 • Curve P-521
	[selection: key size in the table 2 ([8])]	• 256-bit • 384-bit • 521-bit • 256-bit • 384-bit • 521-bit

SFR ID	Selection / Assignment text	Selection / Assignment value
	[selection: standards in the table 2 ([8])]	• RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111] • RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111] • RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111] • FIPS PUB 186-4 B.4 and D.1.2.3 [FIPS PUB 186-4] • FIPS PUB 186-4 B.4 and D.1.2.4 [FIPS PUB 186-4] • FIPS PUB 186-4 B.4 and D.1.2.5 [FIPS PUB 186-4]
FCS_CKM.5.1 [ECKA-EG]	[selection: AES-256, none other]	AES-256
	[selection: elliptic curves in table 2 ([8])]	• brainpoolP256r1 • brainpoolP384r1 • brainpoolP521r1 • Curve P-256 • Curve P-384 • Curve P-521
	[selection:256 bits, none other]	256 bits
FCS_CKM.1.1 [AES_RSA]	[selection: AES-256, none other]	AES-256
	[selection:256 bits, none other]	256 bits
FCS_CKM.5.1 [AES_RSA]	[selection: AES-256, none other]	AES-256
	[selection:256 bits, none other]	256 bits
FCS_COP.1.1 [KW]	[selection: KW, KWP]	KWP
	[selection:256 bits, none other]	256 bits
FCS_COP.1.1 [KU]	[selection: KW, KWP]	KWP
	[selection:256 bits, none other]	256 bits
FPT_ISA.1.5 [CK]	(2) [assignment: additional importation control rules]	none
FPT_ESA.1.4 [CK]	[assignment: additional exportation control rules]	none
FCS_COP.1.1 [ED]	[selection: AES-256, no other algorithm]	AES-256
	[selection: CRT, OFB, CFB, no other]	CRT, OFB, CFB
	[selection: 256 bits, no other key size]	256 bits
FCS_COP.1.1 [HEM]	[selection: FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA, FCS_CKM.5/ECDHE]	FCS_CKM.1/ECKA-EG, FCS_CKM.1/AES_RSA
	[selection: AES-256, none other]	AES-256

SFR ID	Selection / Assignment text	Selection / Assignment value
	[selection: CBC [49], CCM [51], GCM [52]]	CBC [49], CCM [51], GCM [52]
	[selection: CMAC [50], GMAC [52], HMAC [53]]	CMAC [50], GMAC [52], HMAC [53]
	[selection: 256 bits, no other key size]	256 bits
FCS_COP.1.1 [HDM]	[selection: FCS_CKM.5/ ECDHE, FCS_CKM.5/ECKA-EG, FCS_CKM.5/AES_RSA]	FCS_CKM.5/ECKA-EG, FCS_CKM.5/AES_RSA
	[selection: CMAC [50], GCM [52], HMAC [53]]	CMAC [50], GCM [52], HMAC [53]
	[selection: AES-256, none other]	AES-256
	[selection: CBC [49], CCM [51], GMAC [52]]	CBC [49], CCM [51], GMAC [52]
	[assignment: cryptographic key sizes]	256 bits
FCS_COP.1.1 [MAC]	[selection: AES-256, none other]	AES-256
	[selection: GMAC [52], no other]	GMAC [52]
	[selection: 256 bits, no other key size]	256 bits
FCS_COP.1.1 [HMAC]	[selection: HMAC-SHA-1, HMAC-SHA384, no other]	HMAC-SHA-1, HMAC-SHA384
	[assignment: cryptographic key sizes]	from 128 bit to 896 bit in 8 bit steps
FCS_COP.1.1 [CDS-ECDSA]	[selection: elliptic curves in the table 2 ([8])]	• brainpoolP256r1 • brainpoolP384r1 • brainpoolP521r1 • Curve P-256 • Curve P-384 • Curve P-521
	[selection: key size in the table 2 ([8])]	• 256-bit • 384-bit • 521-bit • 256-bit • 384-bit • 521-bit

SFR ID	Selection / Assignment text	Selection / Assignment value
	[selection: standards in the table 2 ([8])]	• RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111] • RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111] • RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111] • FIPS PUB 186-4 B.4 and D.1.2.3 [FIPS PUB 186-4] • FIPS PUB 186-4 B.4 and D.1.2.4 [FIPS PUB 186-4] • FIPS PUB 186-4 B.4 and D.1.2.5 [FIPS PUB 186-4]
FCS_COP.1.1 [VDS-ECDSA]	[selection: elliptic curves in the table 2 ([8])]	• brainpoolP256r1 • brainpoolP384r1 • brainpoolP521r1 • Curve P-256 • Curve P-384 • Curve P-521
	[selection: key size in the table 2 ([8])]	• 256-bit • 384-bit • 521-bit • 256-bit • 384-bit • 521-bit
	[selection: standards in the table 2 ([8])]	• RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111] • RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111] • RFC5639 [RFC5639], TR-03111, section 4.1.3 [TR-03111] • FIPS PUB 186-4 B.4 and D.1.2.3 [FIPS PUB 186-4] • FIPS PUB 186-4 B.4 and D.1.2.4 [FIPS PUB 186-4] • FIPS PUB 186-4 B.4 and D.1.2.5 [FIPS PUB 186-4]
FCS_COP.1.1 [CDS-RSA]	[assignment: cryptographic key sizes]	2000 bit up to 4096 bit in 8 bit steps
FCS_COP.1.1 [VDS-RSA]	[assignment: cryptographic key sizes]	2000 bit up to 4096 bit in 8 bit steps
FDP_DAU.2.1 [Sig]	[selection: FCS_COP.1/CDS-RSA, FCS_COP.1/CDS-ECDSA]	FCS_COP.1/CDS-RSA, FCS_COP.1/CDS-ECDSA
FDP_DAU.2.1 [Att]	[selection: FCS_COP.1/ CDS-RSA, FCS_COP.1/ CDS-ECDSA, ECDAA according to [selection: [54][55]], [assignment: other cryptographic authentication mechanism]]	FCS_COP.1/CDS-RSA, FCS_COP.1/CDS-ECDSA according to respectively RSA and ECDSA digital signature mechanisms

SFR ID	Selection / Assignment text	Selection / Assignment value
FTP_ITC.1.1 [CSP]	[selection: logically separated from other communication channels, using physical separated ports]	logically separated from other communication channels
	[selection: Authentication of TOE and remote entity according to the case in table 4] ([8])	• FIA_API.1/PACE, FIA_UAU.5.1 (2) • FIA_API.1/CA, FIA_UAU.5.1 (4) or (5), and (6)
	[assignment: according to the case in table 4] ([8])	• modfication, disclosure • modfication, disclosure
	[selection: cryptographic operation according to the case in table 4] ([8])	• FCS_COP.1/TCM • FCS_COP.1/TCE
FCS_CKM.1.1 [PACE]	[selection: elliptic curves in the table 2 ([8])]	• brainpoolP256r1 • brainpoolP384r1 • brainpoolP521r1 • Curve P-256 • Curve P-384 • Curve P-521
	[selection: 128 bits, 192 bits, 256 bits]	128 bits, 192 bits, 256 bits
FCS_CKM.1.1 [TCAP]	[selection: 128 bits, 192 bits, 256 bits]	128 bits, 192 bits, 256 bits
FCS_COP.1.1 [TCE]	[selection: CBC [49], CCM [51], GCM [52]]	CBC [49], CCM [51], GCM [52]
	[selection: 128 bits, 192 bits, 256 bits]	128 bits, 192 bits, 256 bits
FCS_COP.1.1 [TCM]	[selection: CMAC [50], GMAC [52]]	CMAC [50], GMAC [52]
	[selection: 128 bits, 192 bits, 256 bits]	128 bits, 192 bits, 256 bits
FMT_MTD.1.1 [RAD]	(1) [selection: Administrator, User Administrator]	User Administrator
	(2) [selection: Administrator, User Administrator]	User Administrator
	(4) [selection: Administrator, User Administrator]	User Administrator
	(5) [assignment: time frame]	time frame chosen by the User Administrator
	(5) [selection: Administrator, User Administrator]	User Administrator
	(6) [selection: Unidentified user, Unauthenticated user]	Unauthenticated user
	(6) [selection: Administrator, User Administrator]	User Administrator

SFR ID	Selection / Assignment text	Selection / Assignment value
FIA_AFL.1.1 [CSP]	[selection: [assignment: positive integer number]number], an [selection: Administrator, User Administrator] configurable positive integer within [assignment: range of acceptable values]]	Administrator configurable positive integer within a range of values determined by this administrator
	[assignment: list of authentication events]	consecutive failed authentication attempt
FIA_AFL.1.2 [CSP]	[assignment: met, surpassed]	met
	[assignment: list of actions]	explicitly delete the password
FMT_SAE.1.1 [CSP]	[selection: Administrator, User Administrator]	User Administrator
FIA_UID.1.1 [CSP]	(3) [assignment: list of other TSF-mediated actions]	none
FIA_UAU.1.1 [CSP]	(3) [selection: a role, a set of role]	a role
	(4) [assignment: list of other TSF-mediated actions]	none
FIA_UAU.5.2 [CSP]	(7) [assignment: additional rules]	none
FIA_UAU.6.1 [CSP]	(4) [assignment: list of other conditions under which re-authentication is required]	none
FDP_ACC.1.1 [Oper]	(1) [selection: Administrator, Crypto-Officer]	Administrator
	(1) [assignment: other roles]	none
FDP_ACF.1.1 [Oper]	(1) [selection: Administrator, Crypto-Officer]	Administrator
	(1) [assignment: other roles]	None
FDP_ACF.1.2 [Oper]	(1) [selection: Administrator, Crypto-Officer]	Administrator
	(3) [assignment: other rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]	none
FDP_ACF.1.3 [Oper]	(1 - Table 5) [selection: Administrator, Crypto-Officer, Key Owner]	Administrator, Key Owner
	(1 - Table 5) [selection: Administrator, Crypto-Officer, Key Owner]	Administrator, Key Owner

SFR ID	Selection / Assignment text	Selection / Assignment value
	(2) [assignment: additional rules, based on security attributes, that explicitly authorise access of subjects to objects]	none
FDP_ACF.1.4 [Oper]	(3) [assignment: additional rules, based on security attributes, that explicitly deny access of subjects to objects]	none
FMT_SMF.1.1 [CSP]	(4) [assignment: additional list of security management functions to be provided by the TSF]	none
FMT_SMR.1.1 [CSP]	[selection: Administrator, Crypto-Officer, User Administrator, Update Agent]	Administrator, User Administrator, Update Agent
	[selection: [assignment: other roles], no other roles]	no other roles
FMT_MSA.2.1 [CSP]	(4) [assignment: additional security attributes]	none
FMT_MOF.1.1 [CSP]	(1) [selection: Administrator, User Administrator]	User Administrator
	(2) [selection: Administrator, User Administrator]	User Administrator
	(3) [selection: Administrator, User Administrator]	User Administrator
	(4) [selection: Administrator, User Administrator]	User Administrator
FDP_SDC.1.1 [CSP]	[assignment: memory area]	NVM
FPT_TST.1.1 [CSP]	[assignment: parts of TSF]	the TSF
FCS_COP.1.1 [VDSUCP]	[assignment: cryptographic algorithm]	ECDSA with NIST P-256, Brainpool P256r1
	[assignment: cryptographic key sizes]	256 bits
	[assignment: list of standards]	FIPS 186-4 [48]
FCS_COP.1.1 [DecUCP]	[assignment: cryptographic algorithm]	AES-128 in CBC mode
	[assignment: cryptographic key sizes]	128 bits
	[assignment: list of standards]	[49]
FDP_ACC.1.1 [UCP]	[selection: Administrator, Update Agent]	Update Agent
FDP_ACF.1.1 [UCP]	[selection: Administrator, Update Agent]	Update Agent

SFR ID	Selection / Assignment text	Selection / Assignment value
FDP_ACF.1.2 [UCP]	(1) [selection: Administrator, Update Agent]	Update Agent
	(2) [selection: Administrator, Update Agent]	Update Agent
	(2) (b) the Version Number of the Update Code Package is equal or higher than the Version Number of the TSF	This statement is covered by a requirement into the UGM [12]
FDP_ACF.1.3 [UCP]	[assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]	None
FDP_ACF.1.4 [UCP]	[assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]	None

7.2 Security Assurance Requirements

The assurance requirements of this evaluation are EAL5 augmented by AVA_VAN.5, ALC_DVS.2, ASE_TSS.2, and ALC_FLR.1. This applies to all PP claimed in Section 2.3.

The assurance requirements ensure, among others, the security of the TOE during its development and production.

7.3 Security Functional Requirements Dependencies

7.3.1 JCOP

Table 63.

Requirements	CC Dependencies	Satisfied dependencies
FCS_RNG.1	No dependencies	
FDP_ACC.1[SD]	FDP_ACF.1 Security attribute based access control	FDP_ACF.1[SD]
FDP_ACC.2[RM]	FDP_ACF.1 Security attribute based access control	FDP_ACF.1[RM]
FDP_ACF.1[SD]	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1[SD] FMT_MSA.3[SD]
FDP_ACF.1[RM]	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.2[RM] FMT_MSA.3[RM]
FDP_ROL.1[CCM]	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]	FDP_ACC.1[SD]
FIA_AFL.1[PIN]	FIA_UAU.1 Timing of authentication	see AppNote in FIA_ AFL.1[PIN]

Requirements	CC Dependencies	Satisfied dependencies
FIA_UID.1[OSU]	No dependencies	
FIA_UID.1[CFG]	No dependencies	
FIA_UID.1[RM]	No dependencies	
FIA_UAU.1[SC]	A_UID.1 Timing of identification	FIA_UID.1[SC]
FIA_UAU.1[RM]	FIA_UID.1 Timing of identification	FIA_UID.1[RM]
FIA_UAU.1[OSU]	FIA_UID.1 Timing of identification	FIA_UID.1[OSU]
FIA_UAU.4[SC]	No dependencies	
FIA_UAU.4[OSU]	No dependencies	
FMT_MSA.1[OSU]	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_IFC.2[OSU] FMT_SMR.1[OSU] FMT_SMF.1[OSU]
FMT_MSA.1[CFG]	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_IFC.2[CFG] FMT_SMR.1[CFG] FMT_SMF.1[CFG]
FMT_MSA.1[SD]	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1[SD] FMT_SMR.1[SD] FMT_SMF.1[SD]
FMT_MSA.1[RM]	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.2[RM] FMT_SMR.1[SD] FMT_SMF.1[RM]
FMT_MSA.3[OSU]	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1[OSU] FMT_SMR.1[OSU]
FMT_MSA.3[CFG]	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1[OSU] FMT_SMR.1[OSU]
FMT_MSA.3[SD]	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1[OSU] FMT_SMR.1[OSU]
FMT_MSA.3[RM]	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1[OSU] FMT_SMR.1[OSU]
FMT_SMF.1[OSU]	No dependencies	
FMT_SMF.1[CFG]	No dependencies	

Requirements	CC Dependencies	Satisfied dependencies
FMT_SMF.1[SD]	No dependencies	
FMT_SMF.1[RM]	No dependencies	
FMT_SMR.1[OSU]	FIA_UID.1 Timing of identification	FIA_UID.1[OSU]
FMT_SMR.1[CFG]	FIA_UID.1 Timing of identification	FIA_UID.1[CFG]
FMT_SMR.1[SD]	FIA_UID.1 Timing of identification	FIA_UID.1[SC]
FPT_EMSEC.1	No dependencies	
FPT_FLS.1[OSU]	No dependencies	
FPT_FLS.1[CCM]	No dependencies	
FPT_PHP.3	No dependencies	

7.3.1.1 JCOP Rationale for Exclusion of Dependencies

The dependency FIA_UID.1 of FMT_SMR.1[INSTALLER] is unsupported. This ST 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 unsupported. This ST 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 unsupported. 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 unsupported. 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 JCVM or other components of the TOE detect these events during their usual working order. Thus, there is no mandatory audit recording in this ST.

The dependency FIA_UAU.1 of FIA_AFL.1[PIN] is unsupported. The TOE implements the firewall access control SFP, based on which access to the object Implementing FIA_AFL.1[PIN] is organized.

7.3.2 eUICC

The Security Functional Requirements dependencies for the eUICC component are strictly the same in the eUICC PP [7].

7.3.3 CSP

The Security Functional Requirements dependencies for the the CSP component are the same in the CSP PP [8] with only the following differences:

- FCS_COP.1[VDSUCP]: the import of UCP signature verification key is done during manufacturing.

- FCS_COP.1.1[DecUCP]: the import of UCP decryption key is done during manufacturing.

7.4 Security Requirements Rationales

7.4.1 Security Assurance Requirements Rationale

The selection of assurance components is based on the following underlying PPs:

- JavaCard [6]
- eUICC [7]
- CSP [8]

The Security Target uses the augmentations from the PP, chooses EAL5 and adds the components AVA_VAN.5 ALC_DVS.2, ASE_TSS.2 and ALC_FLR.1

The rationale for the augmentations is the same as in the PP.

The assurance level EAL5 is an elaborated pre-defined level of the CC, part 3 [3]. The assurance components in an EAL level are chosen in a way that they build a mutually supportive and complete set of components. The additional requirements chosen for augmentation do not add any dependencies, which are not already fulfilled for the corresponding requirements contained in EAL5. Therefore, the components AVA_VAN.5, ALC_DVS.2, ASE_TSS.2 and ALC_FLR.1 and ALC_FLR.1 add additional assurance to EAL5, but the mutual support of the requirements is still guaranteed.

7.4.2 Security Functional Requirements Rationales

7.4.2.1 JCOP

The following rationales of Security Functional Requirements for the JCOP component only covers the modifications regarding the JCOP PP [6] due to additions and refinements in Security Functional Requirements and Security Objectives.

7.4.2.1.1 Execution

7.4.2.1.1.1 OT.OPERATE

Table 64.

SFR	Rationale
FIA_AFL.1[PIN]	Contributes to meet the objective by protecting the authentication.

7.4.2.1.2 Applet Management

7.4.2.1.2.1 OT.APPLI-AUTH

Table 65.

SFR	Rationale
FCS_COP.1	Refinement: applies to FCS_COP.1[DAP]. Contributes to meet the security objective by ensuring that the loaded Executable Application is legitimate by specifying the algorithm to be used in order to verify the DAP signature of the Verification Authority.

SFR	Rationale
FDP_ROL.1[CCM]	Contributes to meet this security objective by ensures that card management operations may be cleanly aborted.
FPT_FLS.1[CCM]	Contributes to meet the security objective by preserving a secure state when failures occur.

7.4.2.1.2.2 OT.DOMAIN-RIGHTS

Table 66.

SFR	Rationale
FDP_ACC.1[SD]	Contributes to cover this security objective by enforcing a Security Domain access control policy (rules and restrictions) that ensures a secure card content management.
FDP_ACF.1[SD]	Contributes to cover this security objective by enforcing a Security Domain access control policy (rules and restrictions) that ensures a secure card content management.
FMT_MSA.1[SD]	Contributes to cover this security objective by enforcing a Security Domain access control policy (rules and restrictions) that ensures a secure card content management.
FMT_MSA.3[SD]	Contributes to cover this security objective by enforcing a Security Domain access control policy (rules and restrictions) that ensures a secure card content management.
FMT_SMF.1[SD]	Contributes to cover this security objective by enforcing a Security Domain access control policy (rules and restrictions) that ensures a secure card content management.
FMT_SMR.1[SD]	Contributes to cover this security objective by enforcing a Security Domain access control policy (rules and restrictions) that ensures a secure card content management.
FTP_ITC.1[SC]	Contributes to cover this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.
FCO_NRO.2[SC]	Contributes to cover this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.
FDP_IFC.2[SC]	Contributes to cover this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.
FDP_IFF.1[SC]	Contributes to cover this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.
FMT_MSA.1[SC]	Contributes to cover this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.
FMT_MSA.3[SC]	Contributes to cover this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.
FMT_SMF.1[SC]	Contributes to cover this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.

SFR	Rationale
FIA_UID.1[SC]	Contributes to cover this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.
FIA_UAU.1[SC]	Contributes to cover this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.
FIA_UAU.4[SC]	Contributes to cover this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.

7.4.2.1.2.3 OT.COMM_AUTH

Table 67.

SFR	Rationale
FCS_COP.1	Contributes to meet the security objective by specifying secure cryptographic algorithm that shall be used to determine the origin of the card management commands.
FMT_SMR.1[SD]	Contributes to meet the security objective by specifying the authorized identified roles enabling to send and authenticate card management commands.
FTP_ITC.1[SC]	Contributes to meet the security objective by ensuring the origin of card administration commands.
FDP_IFC.2[SC]	Contributes to meet the security objective by specifying the authorized identified roles enabling to send and authenticate card management commands.
FDP_IFF.1[SC]	Contributes to meet the security objective by specifying the authorized identified roles enabling to send and authenticate card management commands.
FMT_MSA.1[SC]	Contributes to meet the security objective by specifying security attributes enabling to authenticate card management requests.
FMT_MSA.3[SC]	Contributes to meet the security objective by specifying security attributes enabling to authenticate card management requests.
FIA_UID.1[SC]	Contributes to meet the security objective by specifying the actions that can be performed before authenticating the origin of the APDU commands that the TOE receives.
FIA_UAU.1[SC]	Contributes to meet the security objective by specifying the actions that can be performed before authenticating the origin of the APDU commands that the TOE receives.

7.4.2.1.2.4 OT.COMM_INTEGRITY

Table 68.

SFR	Rationale
FCS_COP.1	Contributes to meet the security objective by by specifying secure cryptographic algorithm that shall be used to ensure the integrity of the card management commands.
FMT_SMR.1[SD]	Contributes to cover this security objective by defining the roles enabling to send and authenticate the card management requests for which the integrity has to be ensured.

SFR	Rationale
FTP_ITC.1[SC]	Contributes to meet the security objective by ensuring the integrity of card management commands.
FDP_IFC.2[SC]	Contributes to cover the security objective by enforcing the Secure Channel Protocol information flow control policy to guarantee the integrity of administration requests.
FDP_IFF.1[SC]	Contributes to cover the security objective by enforcing the Secure Channel Protocol information flow control policy to guarantee the integrity of administration requests.
FMT_MSA.1[SC]	Contributes to cover the security objective by specifying security attributes enabling to guarantee the integrity of card management requests.
FMT_MSA.3[SC]	Contributes to cover the security objective by specifying security attributes enabling to guarantee the integrity of card management requests.
FMT_SMF.1[SC]	Contributes to meet the security objective by specifying the actions activating the integrity check on the card management commands.

7.4.2.1.2.5 OT.COMM_CONFIDENTIALITY

Table 69.

SFR	Rationale
FCS_COP.1	Contributes to meet this objective by specifying secure cryptographic algorithm that shall be used to ensure the confidentiality of the card management commands.
FMT_SMR.1[SD]	Contributes to cover the security objective by defining the roles enabling to send and authenticate the card management requests for which the confidentiality has to be ensured.
FTP_ITC.1[SC]	Contributes to cover the security objective by ensuring the confidentiality of card management commands.
FDP_IFC.2[SC]	Contributes to cover the security objective by enforcing the Secure Channel Protocol information flow control policy to guarantee the confidentiality of administration requests.
FDP_IFF.1[SC]	Contributes to cover the security objective by enforcing the Secure Channel Protocol information flow control policy to guarantee the confidentiality of administration requests.
FMT_MSA.1[SC]	Contributes to cover the security objective by specifying security attributes enabling to guarantee the confidentiality of card management requests by decrypting those requests and imposing management conditions on that attributes.
FMT_MSA.3[SC]	Contributes to cover the security objective by specifying security attributes enabling to guarantee the confidentiality of card management requests by decrypting those requests and imposing management conditions on that attributes.
FMT_SMF.1[SC]	Contributes to cover the security objective by specifying the actions ensuring the confidentiality of the card management commands.

7.4.2.1.3 Card Management

7.4.2.1.3.1 OT.CARD-MANAGEMENT

Table 70.

SFR	Rationale
FDP_ACC.2[ADEL]	Contributes to meet the objective by the ADEL access control policy which ensures the non-introduction of security holes. The integrity and confidentiality of data that does not belong to the deleted applet or package is a by-product of this policy as well.
FDP_ACF.1[ADEL]	Contributes to meet the objective by the ADEL access control policy which ensures the non-introduction of security holes. The integrity and confidentiality of data that does not belong to the deleted applet or package is a by-product of this policy as well.
FDP_RIP.1[ADEL]	Contributes to meet the objective by ensuring the non-accessibility of deleted data.
FMT_MSA.1[ADEL]	Contributes to meet the objective by enforcing the ADEL access control SFP.
FMT_MSA.3[ADEL]	Contributes to meet the objective by enforcing the ADEL access control SFP.
FMT_SMR.1[ADEL]	Contributes to meet the objective by maintaing the role applet deletion manager.
FPT_ RCV.3[INSTALLER]	Contributes to meet the objective by protecting the TSFs against possible failures of the deletion procedures.
FPT_ FLS.1[INSTALLER]	Contributes to meet the objective by protecting the TSFs against possible failures of the installer.
FPT_FLS.1[ADEL]	Contributes to meet the objective by protecting the TSFs against possible failures of the deletion procedures.
FDP_UIT.1[CCM]	Contributes to meet the objective by enforcing the Secure Channel Protocol information flow control policy and the Security Domain access control policy which controls the integrity of the corresponding data.
FDP_ROL.1[CCM]	Contributes to meet this security objective by ensures that card management operations may be cleanly aborted.
FDP_ITC.2[CCM]	Contributes to meet the security objective by enforcing the Firewall access control policy and the Secure Channel Protocol information flow policy when importing card management data.
FPT_FLS.1[CCM]	Contributes to meet the security objective by preserving a secure state when failures occur.
FDP_ACC.1[SD]	Contributes to cover this security objective by enforcing a Security Domain access control policy (rules and restrictions) that ensures a secure card content management.
FDP_ACF.1[SD]	Contributes to cover this security objective by enforcing a Security Domain access control policy (rules and restrictions) that ensures a secure card content management.
FMT_MSA.1[SD]	Contributes to cover this security objective by enforcing a Security Domain access control policy (rules and restrictions) that ensures a secure card content management.

SFR	Rationale
FMT_MSA.3[SD]	Contributes to cover this security objective by enforcing a Security Domain access control policy (rules and restrictions) that ensures a secure card content management.
FMT_SMF.1[SD]	Contributes to cover this security objective by enforcing a Security Domain access control policy (rules and restrictions) that ensures a secure card content management.
FMT_SMR.1[SD]	Contributes to cover this security objective by enforcing a Security Domain access control policy (rules and restrictions) that ensures a secure card content management.
FTP_ITC.1[SC]	Contributes to meet this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.
FCO_NRO.2[SC]	Contributes to meet this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.
FDP_IFC.2[SC]	Contributes to meet this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.
FDP_IFF.1[SC]	Contributes to meet this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.
FMT_MSA.1[SC]	Contributes to meet this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.
FMT_MSA.3[SC]	Contributes to meet this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.
FMT_SMF.1[SC]	Contributes to meet this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.
FIA_UID.1[SC]	Contributes to meet this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.
FIA_UAU.1[SC]	Contributes to meet this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.
FIA_UAU.4[SC]	Contributes to meet this security objective by enforcing Secure Channel Protocol information flow control policy that ensures the integrity and the authenticity of card management operations.

7.4.2.1.4 Smart Card Platform

7.4.2.1.4.1 OT.SCP.IC

SFR	Rationale
FAU_ARP.1	Contributes to the coverage of the objective by resetting the card session or terminating the card in case of physical tampering.
FPR_UNO.1	Contributes to the coverage of the objective by ensuring leakage resistant implementations of the unobservable operations.

SFR	Rationale
FPT_EMSEC.1	Contributes to meet the objective.
FPT_PHP.3	Contributes to the coverage of the objective by preventing bypassing, deactivation or changing of other security features.

7.4.2.1.4.2 OT.SCP.RECOVERY

SFR	Rationale
FAU_ARP.1	Contributes to the coverage of the objective by ensuring reinitialization of the Java Card System and its data after card tearing and power failure.
FPT_FLS.1	Contributes to the coverage of the objective by preserving a secure state after failure.

7.4.2.1.4.3 OT.SCP.SUPPORT

SFR	Rationale
FCS_CKM.1	Contributes to meet the objective.
FCS_CKM.4	Contributes to meet the objective.
FCS_COP.1	Contributes to meet the objective.
FDP_ ROL.1[FIREWALL]	Contributes to meet the objective.

7.4.2.1.4.4 OT.IDENTIFICATION

SFR	Rationale
FAU_SAS.1[SCP]	Covers the objective.The Initialisation Data (or parts of them) are used for TOE identification

7.4.2.1.5 Random Numbers

7.4.2.1.5.1 OT.RND

Table 71.

SFR	Rationale
FCS_RNG.1	Covers the objective by providing random numbers of good quality by specifying class DRG.3 of AIS 20. It was chosen to define FCS_RNG.1 explicitly, because Part 2 of the Common Criteria does not contain generic security functional requirements for Random Number generation. (Note that there are security functional requirements in Part 2 of the Common Criteria, which refer to random numbers. However, they define requirements only for the authentication context, which is only one of the possible applications of random numbers).

7.4.2.1.6 Config Applet

7.4.2.1.6.1 OT.CARD-CONFIGURATION

Table 72.

SFR	Rationale
FDP_IFC.2[CFG]	Contributes to meet the objective by controlling the ability to modify configuration items.
FDP_IFF.1[CFG]	Contributes to meet the objective by controlling the ability to modify configuration items.
FMT_MSA.3[CFG]	Contributes to meet the objective by controlling the ability to modify configuration items.
FMT_MSA.1[CFG]	Contributes to meet the objective by controlling the ability to modify configuration items.
FMT_SMR.1[CFG]	Contributes to meet the objective by controlling the ability to modify configuration items.
FMT_SMF.1[CFG]	Contributes to meet the objective by controlling the ability to modify configuration items.
FIA_UID.1[CFG]	Contributes to meet the objective by requiring identification before modifying configuration items.

7.4.2.1.7 OS Update

7.4.2.1.7.1 OT.CONFID-UPDATE-IMAGE.LOAD

Table 73.

SFR	Rationale
FPR_UNO.1	Contributes to the coverage of the objective by ensuring the unobservability of the S.OSU decryption key.
FIA_UID.1[OSU]	Contributes to the coverage of the objective by requiring identification.
FIA_UAU.1[OSU]	Contributes to the coverage of the objective by requiring authentication.

7.4.2.1.7.2 OT.AUTH-LOAD-UPDATE-IMAGE

Table 74.

SFR	Rationale
FDP_IFC.2[OSU]	Contributes to the coverage of the objective by applying the rules of the Information Flow Control policy.
FDP_IFF.1[OSU]	Contributes to the coverage of the objective by applying the rules of the Information Flow Control policy.
FMT_MSA.3[OSU]	Contributes to the coverage of the objective by enforcing restrictive default values for the attributes of the OS Update information flow control SFP.
FMT_SMR.1[OSU]	Contributes to the coverage of the objective by letting S.OSU handle the OS Update procedure.
FIA_UID.1[OSU]	Contributes to the objective by requiring identification of the authorized images.

SFR	Rationale
FIA_UAU.1[OSU]	Contributes to the objective by requiring authentication of the authorized images.

7.4.2.1.7.3 OT.SECURE_LOAD_ACODE

Table 75.

SFR	Rationale
FDP_IFC.2[OSU]	Contributes to the coverage of the objective by ensuring that only allowed versions of the D.UPDATE_IMAGE are accepted and by checking the evidence data of authenticity and integrity.
FMT_SMR.1[OSU]	Contributes to the coverage of the objective by letting S.OSU handle the OS Update procedure.
FPT_FLS.1[OSU]	Contributes to the coverage of the objective by ensuring a secure state after interruption of the OS Update procedure (Load Phase).
FIA_UAU.4[OSU]	Contributes to meet the objective by enforcing authenticity and integrity of D.UPDATE_IMAGE (i.e. Additional Code).

7.4.2.1.7.4 OT.SECURE_AC_ACTIVATION

Table 76.

SFR	Rationale
FMT_MSA.1[OSU]	Contributes to the coverage of the objective by allowing to modify the Current Sequence Number only after successful OS Update procedure.
FMT_SMR.1[OSU]	Contributes to the coverage of the objective by letting S.OSU handle the OS Update procedure.
FMT_SMF.1[OSU]	Contributes to the objective by providing information on the currently activated software (Current Sequence Number).
FPT_FLS.1[OSU]	Contributes to the coverage of the objective by ensuring atomicity of the OS Update procedure (Load Phase).

7.4.2.1.7.5 OT.TOE_IDENTIFICATION

Table 77.

SFR	Rationale
FDP_SDI.2	Contributes to cover the objective by storing the identification data (D.TOE_IDENTIFICATION) in an integrity protected store.
FMT_SMF.1[OSU]	Contributes to cover the objective by providing the ability to query the identification data (Current Sequence Number, Reference Sequence Number, Final Sequence Number) of the TOE.

7.4.2.1.8 Restricted Mode

7.4.2.1.8.1 OT.ATTACK-COUNTER

Table 78.

SFR	Rationale
FMT_SMR.1[SD]	Contributes to cover the objective by defining the security role ISD.

SFR	Rationale
FMT_MSA.3[RM]	Contributes to cover the objective by restricting the initial value of the Attack Counter and allowing nobody to change the initial value.
FMT_MSA.1[RM]	Contributes to cover the objective by only allowing the ISD to modify the Attack Counter.
FIA_UAU.1[RM]	Contributes to cover the objective by requiring authentication before resetting the Attack Counter.
FIA_UID.1[RM]	Contributes to cover the objective by requiring identification before resetting the Attack Counter.

7.4.2.1.8.2 OT.RESTRICTED-MODE

Table 79.

SFR	Rationale
FMT_SMR.1[SD]	Contributes to cover the objective by defining the security role ISD.
FDP_ACC.2[RM]	Contributes to the coverage of the objective by defining the subject of the Restricted Mode access control SFP.
FDP_ACF.1[RM]	Contributes to cover the objective by controlling access to objects for all operations.
FMT_SMF.1[RM]	Contributes to cover the objective by defining the management functions of the restricted mode.
FIA_UAU.1[RM]	Contributes to cover the objective by requiring authentication before resetting the Attack Counter.
FIA_UID.1[RM]	Contributes to cover the objective by requiring identification before resetting the Attack Counter.

7.4.2.2 eUICC

The rationale of Security Functional Requirements for the the eUICC component is strictly the same as in the eUICC PP [7].

7.4.2.3 CSP

The rationale of Security Functional Requirements for the CSP component is strictly the same as in the CSP PP [8].

8 TOE summary specification (ASE_TSS)

8.1 Introduction

The Security Functions (SF) introduced in this section realize the SFRs of the TOE. See Table 8.1 for list of all Security Functions. Each SF consists of components spread over several TOE modules to provide a security functionality and fulfill SFRs.

8.2 Security Functionality

8.2.1 JCOP

SF.JCVM	**Java Card Virtual Machine** SF.JCVM provides the Java Card Virtual Machine including byte code interpretation and the Java Card Firewall according to the specifications [24] and [25]. This fulfills the SFRs FDP_IFC.1[JCVM], FDP_IFF.1[JCVM], FMT_SMF.1, FMT_SMR.1, FDP_ROL.1[FIREWALL], FDP_ACF.1[FIREWALL], FDP_ACC.2[FIREWALL] and FIA_UID.2[AID]. SF.JCVM supports FAU_ARP.1 and FPT_FLS.1 by throwing Java Exceptions according to these specifications. Additionally it supports these SFRs by verification of the integrity of used Java object headers. Security attributes in SF.JCVM are separated from user data and not accessible by applets to fulfill FMT_MSA.1[JCRE] and FMT_MSA.1[JCVM]. All values for security attributes are initialized and assigned by the system itself which fulfills FMT_MSA.2[FIREWALL-JCVM], FMT_MSA.3[FIREWALL], and FMT_MSA.3[JCVM]. The full Java Card implementation is then controlled by this mechanism including GlobalPlatform GlobalPlatform Amendments A [28], B [29], C [31], D [32], E [33], F [34], H [35] and I [36]. SF.JCVM ensures together with SF.PERS_MEM that the system is halted in case non existing Java objects could be referenced after an aborted transaction to fulfill FDP_RIP.1[ABORT].
SF.CONFIG	**Configuration Management** SF.CONFIG provides means to store Initialization Data and Pre-personalization Data before TOE delivery FAU_SAS.1[SCP]. SF.CONFIG provides means to change configurations of the card. Some configurations can be changed by the customer and some can only be changed by NXP (FDP_IFC.2[CFG], FDP_IFF.1[CFG], FMT_MSA.3[CFG], FMT_MSA.1[CFG], FMT_SMR.1[CFG], FMT_SMF.1[CFG], FIA_UID.1[CFG]). SF.CONFIG supports FCS_COP.1 by configuring the behavior of cryptographic operations. Additionally, SF.CONFIG provides proprietary commands to select (FIA_UID.1[SC]) the OS update mechanism SF.OSU and to reset the OS to an initial state (FAU_ARP.1 and FPT_FLS.1).

SF.OPEN	**Card Content Management** SF.OPEN provides the card content management functionality according the GlobalPlatform Specification [26] and GlobalPlatform Amendments A [28], B [29], C [31], D [32], E [33] and F [34]. This supports FCO_NRO.2[SC], FDP_ACC.1[SD], FDP_ACF.1[SD], FDP_UIT.1[CCM], FDP_IFF.1[SC], FDP_IFC.2[SC], FIA_UID.1[SC], FIA_UID.2[AID], FIA_USB.1[AID], FMT_MSA.1[SC], FMT_MSA.1[SD], FMT_MSA.3[SC], FMT_MSA.3[SD], FMT_SMF.1[ADEL], FMT_SMR.1[SD], FMT_SMF.1[SC], FMT_SMF.1[SD], FTP_ITC.1[SC], FMT_MSA.3[ADEL], FMT_SMR.1[INSTALLER], FMT_SMR.1[ADEL], FDP_ITC.2[CCM], FDP_ROL.1[CCM], FIA_UAU.1[SC], FIA_UAU.4[SC], FTP_ITC.1[SC] and FCS_COP.1 (for DAP verification). In addition to the GP specification, the Java Card Runtime Environment specification [25] is followed to support FDP_ACC.2[ADEL], FDP_ACF.1[ADEL], FMT_MSA.3[SC], FMT_MSA.3[SD], FMT_MTD.1[JCRE], FMT_MTD.3[JCRE], FPT_FLS.1[INSTALLER], FDP_RIP.1[bArray], FDP_RIP.1[ADEL], FPT_TDC.1, FPT_FLS.1[ADEL], and FPT_FLS.1[CCM] for application loading, installation, and deletion. AID management is provided by SF.OPEN according to the GlobalPlatform Specification [26], the Java Card Runtime Environment Specification [25], and the Java Card API Specification [23] to support FIA_ATD.1[AID]. SF.OPEN is part of the TOE runtime environment and thus separated from other applications to fulfill FMT_MSA.1[ADEL]. It supports FAU_ARP.1 and FPT_FLS.1 by responding with error messages and fulfills FPT_RCV.3[INSTALLER] by inherent memory cleanup in case of aborted loading and installation.
SF.CRYPTO	**Cryptographic Functionality** SF.CRYPTO provides key creation, key management, key deletion and cryptographic functionality. It provides the API in accordance to the Java Card API Specification [23] to fulfill FCS_CKM.1, FCS_CKM.4, and FCS_COP.1. Proprietary solutions (e.g., key lengths not supported by the Java Card API) are supported following the Java Card API. SF.CRYPTO uses SF.DATA_STORAGE to support FCS_CKM.1, FCS_CKM.4, FDP_RIP.1[KEYS], and FDP_SDI.2[DATA]. The Security Software certified with the TOE hardware supports FCS_COP.1 and FPR_UNO.1. This TSF enforces protection of Key material during cryptographic functions processing and Key Generation, against state-of-the-art attacks, including IC power consumption analysis (FPT_EMSEC.1).
SF.RNG	**Random Number Generator** SF.RNG provides secure random number generation to fulfill FCS_CKM.1 and FCS_RNG.1. Random numbers are generated by the Security Software certified with the TOE hardware. SF.RNG provides an API according to the Java Card API Specification [23] to generate random numbers according to FCS_RNG.1.
SF.DATA_STORAGE	**Secure Data Storage** SF.DATA_STORAGE provides a secure data storage for confidential data. It is used to store cryptographic keys (supports FCS_CKM.1 and FCS_CKM.4) and to store PINs (supports FIA_AFL.1[PIN]). All data stored by SF.DATA_STORAGE is CRC32 integrity protected to fulfill FDP_SDI.2[DATA], FAU_ARP.1, and FPT_FLS.1. The stored data is AES encrypted to fulfill FPR_UNO.1.

SF.OSU	**Operating System Update** SF.OSU provides secure functionality to update the JCOP5.2 OS or UpdaterOS itself with an image created by a trusted off-card entity (FMT_SMR.1[OSU], FMT_SMF.1[OSU]). SF.OSU allows an authenticated OSU command (FIA_UAU.4[OSU]) to upload an integrity and confidentiality protected update image to update to another operating system version(FDP_IFC.2[OSU], FDP_IFF.1[OSU]). User authentication is based on the verification of signed OSU commands to fulfill FIA_UAU.1[OSU] and FIA_UID.1[OSU]. Integrity protection of OSU commands uses ECDSA, SHA-256 and CRC verification to fulfill FDP_IFF.1[OSU]. Confidentiality of the update image is ensured by ECDH and AES encryption to fulfill FDP_IFF.1[OSU]. SF.OSU ensures that the system stays in a secure state in case of invalid or aborted update procedures to fulfill FPT_FLS.1[OSU] and ensures that the information identifying the currently running OS is modified and the updated code is activated only after successfull OS Update procedure FMT_MSA.3[OSU], FMT_MSA.1[OSU]. CSP requirements are covered as well: • Access control and transfer conditions FDP_ITC.2[UCP], FPT_TDC.1[UCP], FDP_ACC.1[UCP] and FDP_ACF.1[UCP] are covered as FDP_IFC.2[OSU], FDP_IFF.1[OSU], FIA_UID.1[OSU], FIA_UAU.1[OSU] and FIA_UAU.4[OSU] as those ones cover same requirements on package reception handling: authenticity verification, decryption, version (sequence number in the current product). • FCS_COP.1[VDSUCP] and FCS_COP.1[DecUCP] requirements are covered by the ECDH and ECDSA for signature verification, and by AES encryption. • FDP_RIP.1[UCP] is covered as FDP_RIP.1[TRANSIENT]
SF.OM	**Java Object Management** SF.OM provides the object management for Java objects which are processed by SF.JCVM. It provides object creation (FDP_RIP.1[OBJECTS]) and garbage collection according to the Java Card Runtime Environment Specification [25] to fulfill FDP_RIP.1[ODEL] and FPT_FLS.1[ODEL]. SF.OM throws an Java Exception in case an object cannot be created as requested due to too less available memory. This fulfills FAU_ARP.1 and FPT_FLS.1.
SF.MM	**Memory Management** SF.MM provides deletion of memory for transient arrays, global arrays, and logical channels according to the Java Card Runtime Environment Specification [25]. Thus, it fulfills FDP_RIP.1[TRANSIENT] by granting access to and erasing of CLEAR_ON_RESET and CLEAR_ON_DESELECT transient arrays. It supports FIA_ATD.1[AID] when using logical channels and it fulfills FDP_RIP.1[APDU] and FDP_RIP.1[bArray] by clearing the APDU buffers for new incoming data and by clearing the bArray during application installation.
SF.PIN	**PIN Management** SF.PIN provides secure PIN management by using SF.DATA_STORAGE for PIN objects specified in the Java Card API Specification [23] and the GlobalPlatform Specification [30]. Thus, it fulfills FDP_SDI.2[DATA], FIA_AFL.1[PIN], and FPR_UNO.1.

SF.PERS_MEM	**Persistent Memory Management** SF.PERS_MEM provides atomic write operations and transaction management according to the Java Card Runtime Environment Specification [25]. This supports FAU_ARP.1, FPT_FLS.1, and FDP_ROL.1[FIREWALL]. SF.PERS_MEM supports FDP_RIP.1[ABORT] together with SF.JCVM by halting the system in case of object creation in aborted transactions. Low level write routines to persistent memory in SF.PERS_MEM perform checks for defect memory cells to fulfill FAU_ARP.1 and FPT_FLS.1.
SF.EDC	**Error Detection Code API** SF.EDC provides an Java API for user applications to perform high performing integrity checks based on a checksum on Java arrays [10]. The API throws a Java Exception in case the checksum in invalid. This supports FAU_ARP.1 and FPT_FLS.1.
SF.HW_EXC	**Hardware Exception Handling** SF.HW_EXC provides software exception handler to react on unforeseen events captured by the hardware (hardware exceptions). SF.HW_EXC catches the hardware exceptions, to ensure the system goes to a secure state to fulfill FAU_ARP.1 and FPT_FLS.1, as well as to increase the attack counter in order to resist physical manipulation and probing to fulfill FPT_PHP.3.
SF.RM	**Restricted Mode** SF.RM provides a restricted mode that is entered when the Attack Counter reaches its limit. In restricted mode only limited functionality is available. Only the issuer is able to reset the Attack Counter to leave the restricted mode. This supports FDP_ACC.2[RM], FDP_ACF.1[RM], FMT_MSA.3[RM], FMT_MSA.1[RM], and FMT_SMF.1[RM]. SF.RM only allows a limited set of operations to not identified and not authenticated users when in restricted mode. All other operations require identification and authentication (FIA_UID.1[RM], FIA_UAU.1[RM]).
SF.PID	**Platform Identification** SF.PID provides a platform identifier. For elements that can be identified see 1.8. This feature supports FAU_SAS.1.1[SCP] by using initialization data that is used for platform identification.
SF.SMG_NSC	**No Side-Channel** The TSF ensures that during command execution there are no usable variations in power consumption (measurable at e.g. electrical contacts) or timing (measurable at e.g. electrical contacts) that might disclose cryptographic keys or PINs. All functions of SF.CRYPTO except for SHA are resistant to side-channel attacks (e.g. timing attack, SPA, DPA, DFA, EMA, DEMA) (see FPR_UNO.1 and FPT_EMSEC.1).

8.2.2 eUICC

SF.CRYPTO_eUICC	**eUICC specific cryptographic algorithms** This TSF provides key creation, key management, key deletion and cryptographic functionality specific to the eUICC component. It provides the API in accordance to eUICC specification [38], [39] to fulfill 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], and FCS_COP.1[Mobile_network]. 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 (FPT_EMSEC.1).
SF.ACCESS_eUICC	**eUICC features access protection** This TSF handles the access to eUICC features by external or local users. It based on JavaCard and GlobalPlatform features to implement the different flow controls (FDP_IFC.1[SCP], FDP_IFF.1[SCP], FDP_IFC.1[Platform_services], FDP_IFF.1[Platform_services], FPT_FLS.1[Platform_services]), access control (FDP_ACC.1[ISDR], FDP_ACF.1[ISDR], FDP_ACC.1[ECASD], FDP_ACF.1[ECASD]) and related dependencies (FMT_MSA.1[PLATFORM_DATA], FMT_MSA.1[PPR], FMT_MSA.1[CERT_KEYS], FMT_SMF.1[eUICC], FMT_SMR.1[eUICC], FMT_MSA.1[RAT], FMT_MSA.3[eUICC]), as well as the conditions realization granting the access: identification/ authentication of users (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]) and the different trusted channels establishment (FTP_ITC.1[SCP], FDP_ITC.2[SCP], FPT_TDC.1[SCP], FDP_UCT.1[SCP], FDP_UIT.1[SCP]) in compliance with [38] [39] .
SF.SELF-PROTECTION_eUICC	**eUICC specific self-protections** This TSF extends the scope of self-protections features provided by the JavaCard platform to the eUICC component needs (FDP_SDI.1[eUICC], FDP_RIP.1[eUICC], FPT_FLS.1[eUICC]).

8.2.3 CSP

SF.CRYPTO_CSP	**CSP specific cryptography** This TSF provides key creation, key management, key deletion and cryptographic functionality specific to the CSP component. It provides the API in accordance to CSP specification [43] to fulfill FCS_CKM.1[AES], FCS_CKM.5[AES], FCS_CKM.1[ECC], FCS_CKM.5[ECC], FCS_CKM.1[RSA], FCS_CKM.5[ECDHE], FCS_CKM.1[ECKA-EG], FCS_CKM.5[ECKA-EG], FCS_CKM.1[AES-RSA], FCS_CKM.5[AES-RSA], FCS_COP.1[Hash], FCS_COP.1[KW], FCS_COP.1[KU], FCS_COP.1[ED], FCS_COP.1[HEM], FCS_COP.1[HDM], FCS_COP.1[MAC], FCS_COP.1[HMAC], FCS_COP.1[CDS-ECDSA], FCS_COP.1[VDS-ECDSA], FCS_COP.1[CDS-RSA], FCS_COP.1[VDS-RSA], FCS_COP.1[TCE], FCS_COP.1[TCM], FCS_CKM.1[PACE], FCS_CKM.1[TCAP]. All those are implemented in the JCOP platform. The specific storage of keys requested by FDP_SDC.1[CSP] is covered by AES encryption implemented provided by the JCOP platform.

SF.ACCESS_CSP	**CSP access protection features** This TSF handles the access to CSP features by external or local users. It bases on JavaCard and GlobalPlatform features to implement different access control (FDP_ACC.1[Oper], FDP_ACF.1[Oper], DP_ACC.1[KM]) and the conditions realization granting the access: identification/ authentication of users (FIA_ATD.1[CSP], FIA_AFL.1[CSP], FIA_ USB.1[CSP], FIA_UID.1[CSP], FIA_UAU.1[CSP], FIA_UAU.5[CSP], FIA_UAU.6[CSP], FIA_API.1[CA], FIA_API.1[PACE]) and trusted channels establishment (FTP_ITC.1[CSP]). Related security attributes and data are also based on JavaCard features (FMT_SMF.1[CSP], FMT_SMR.1[CSP], FMT_MOF.1[CSP], FMT_MSA.1[KM], FMT_MSA.2[CSP], FMT_MSA.3[KM], FMT_ MTD.1[KM], FMT_MTD.1[RAD], FMT_MTD.1[RK], FMT_MTD.3[CSP], FMT_SAE.1[CSP])
SF.SERVICES_CSP	**CSP other services** This TSF handles other services as generation of data validity evidences (FDP_DAU.2[Att], FDP_DAU.2[Sig]), exchanges of cryptographic keys (FPT_TDC.1[CK], FPT_TCT.1[CK], FPT_TIT.1[CK], FPT_ISA.1[CK], FPT_ESA.1[CK]), exchanges of certificates (FPT_TDC.1[Cert]), FPT_ TIT.1[Cert], FPT_ISA.1[Cert]) and exchanges of user data (FDP_ ETC.1[CSP], FDP_ETC.2[CSP], FDP_ITC.2[UD]).
SF.SELF-PROTECTION_CSP	**CSP specific self-protections** This TSF extends the scope of self-protections features provided by the JavaCard platform to the CSP component needs (FPT_FLS.1[CSP], FRU_FLT.2[CSP]).

8.3 Protection against Interference and Logical Tampering

The protection of JCOP5.2 against Interference and Logical Tampering is implemented in software within the TOE and supported by the hardware of the micro controller.

The software protection of the TOE makes use of software security services which allow to detect and react on manipulation of the TOE. Two types of reactions are used: If invalid data from outside the TOE is detected then it is assumed that the TOE was used in a wrong way. This is indicated by an appropriate Status Word or Exception. Detected deviations from the physical operating conditions and inconsistencies of internal states and program flow however are considered to be an attack to the TOE. In such cases an internal Attack Counter is increased. Once the Attack Counter reaches the maximum value, the TOE will go into Restricted Mode.

Typical software security mechanisms implemented in the TOE are e.g.:

- Complex patterned values are used instead of boolean values which are sensible to tampering (only one bit needs to be changed to manipulate a false into a true).
- Small random delays are inserted in the program flow to make successful physical interfering more difficult.
- Secret information like Keys or PINs are stored encrypted in the TOE. The Masterkey to decrypt these is not accessible during normal operation.
- Critical data is read after it has been written to non volatile memory.
- Enhanced cryptographic support is based on the certified Security Software for DES, AES, ECC and RSA including protection against fault injection and random number generation.
- Critical values (like PINs) are compared timing-invariant. This prevents from side channel attacks.

A full list of software countermeasures is contained in ADV_ARC.

Further protection against Tampering and Logical Interference is realized by the MMU implemented in hardware. The MMU is able to perform access control to all types of memory. The special function registers access can be restricted by the bridges between the CPU and the peripherals.

JCOP5.2 defines several MMU contexts which restrict access to memory areas. The Master key is stored in specific coprocessor registers and blocked for reading/writing during JCOP operation. Additionally Interference and Logical Tampering is prevented by hardware security services. JCOP5.2 OS runs on a certified smart card HW platform which protects against bypass by physical and logical means such as:

- cryptographic coprocessors (for symmetric and asymmetric cryptography) protected against DPA and DFA,
- enhanced security sensors for clock frequency range, low and high temperature sensor, supply voltage sensors Single Fault Injection (SFI) attack detection, light sensors, and
- encryption of data stored in persistent and transient memory.

8.4 Protection against Bypass of Security Related Actions

JCOP5.2 prevents bypassing security related actions by several software counter measures. Different mechanisms are used depending on the software environment.

Generally all input parameter are validated and in case of incorrect parameters the program flow is interrupted. Such event is indicated by an appropriate Status Word or Exception. This prevents the TOE from being attacked by undefined or unauthorized commands or data.

Basic protection is contributed by implementation of following standards within the TOE:

- Java Applets are separated from each other as defined in the Java Card specifications [23], [24] and [25]. The separation is achieved by implementation of the firewall which prevents Applets to access data belonging to a different Java Card context. Sharing information between different contexts is possible by supervision of the well defined Java Card Firewall mechanism implemented in the TOE.
- Access to security relevant Applications in the TOE (like Security Domains) is protected by the Secure Channel mechanism defined by Global platform [30]. The secure channel allows access to Applications only if the secret keys are known. Further protection implemented in JCOP5.2 prevents brute force attacks to the secret keys of the Secure Channel.

The following mechanisms ensure that it is not possible to access information from the Java Layer without being authorized to do so.

- Status informations like Life Cycle of Applets or the Authentication State of a Secure Channel are stored in complex patterned values which protects them from manipulation.
- Correct order of Java Card Byte Code execution is ensured by the Virtual Machine which detects if Byte Code of a wrong context is executed.
- Correct processing of Byte Codes is ensured by checking at the beginning and end of Byte Code execution that the same Byte Code is executed.

Further protection is achieved by using different buffers for APDUs in case more than one physical interface is supported. This prevents bypassing the state machine on one physical interface by the other interface.

9 Bibliography

9.1 Evaluation documents

[1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, CCMB-2017-04-001, April 2017.

[2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1, Revision 5, CCMB-2017-04-002, April 2017.

[3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1, Revision 5, CCMB-2017-04-003, April 2017.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1, Revision 5, CCMB-2017-04-004, April 2017.

[5] Security IC Platform Protection Profile with Augmentation Packages, Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-CC-PP-0084-2014, Version 1.0, 13 January 2014.

[6] Published by Oracle. Java card protection profile - open configuration, version 3.0.5 (dec 2017), published by oracle, inc. (bsi-cc-pp-0099-2017).

[7] GSMA SGP.25 Embedded UICC for Consumer Devices, GSMA Association, 05 June 2018 (BSI-CC-PP-0100-2018).

[8] BSI. Common Criteria Protection Profile Cryptographic Service Provider, 19 February 2019 (BSI-CC-PP-0104).

[9] Joint Interpretation Library. Joint Interpretation Library, Security requirements for post-delivery code loading, Draft Version 1.0, February 2016.

9.2 Developer documents

[10] NXP. JCOP 5.2 R1.01.1, User Guidance Manual, Rev. 1.8.

[11] NXP. JCOP 5.2 R1.01.1, User Guidance Addendum SEMS, Rev. 1.1.

[12] NXP. JCOP 5.2 R1.01.1, User Guidance Manual Addendum for CSP API, Rev. 1.6.

[13] NXP. JCOP 5.2 R2, User Guidance Manual, Rev. 1.3, doc. no 608813, 8 June, 2020.

[14] NXP. JCOP 5.2 R2, User Guidance Addendum SEMS, Rev. 1.2, doc. no. 614012, 8 June, 2020.

[15] NXP. JCOP 5.2, User Guidance Manual Addendum for CSP API, revision 1.2, doc. no. 614112, 8 June, 2020.

[16] NXP. JCOP 5.2 R2.03.1, User Guidance Manual, Doc 638010, Rev. 1.0, 18 Sept 2020.

[17] NXP. JCOP 5.2 R2.03, User Guidance Manual Addendum for CSP API, Doc 638110, Rev. 1.0, 16 Sept 2020.

[18] NXP. JCOP 5.2 R2.03.1, User Guidance Addendum for SEMS API, Doc 638310, Rev. 1.0, 16 Sept 2020.

[19] NXP. JCOP 5.2 R3.01.1, User Guidance Manual , Doc 622011, Rev. 1.1, 03 May 2021 .

[20] NXP. JCOP 5.2 R3.01, User Guidance Manual Addendum for CSP API , Doc 622110, Rev. 1.0, 15 Jan 2021.

[21] NXP. JCOP 5.2 R3.01.1, User Guidance Addendum for SEMS API , Doc 622210, Rev. 1.0, 15 Jan 2021.

[22] NXP. SN100 Series - Secure Element with Crypto Library, Security Target, NXP Semiconductors, Revision 3.5, 21 April 2021.

9.3 Standards

[23] Published by Oracle. Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0 up to 3.0.5.

[24] Published by Oracle. Java Card 3 Platform, Virtual Machine Specification, Classic Edition, Version 3.0 up to 3.0.5.

[25] Published by Oracle. Java Card 3 Platform, Runtime Environment Specification, Classic Edition, Version 3.0 up to 3.0.5.

[26] GlobalPlatform. GlobalPlatform Card Specification 2.3.1, GPC_SPE_034, GlobalPlatform Inc., Mar 2018.

[27] GlobalPlatform. Confidential Card Content Management, GlobalPlatform Card Specification v2.2 - Amendment A v1.0.1, January 2011.

[28] GlobalPlatform. Confidential Card Content Management - Amendment A v1.1, Nov 2015.

[29] GlobalPlatform. Remote Application Management over HTTP - Amendment B v1.1.3, May 2015.

[30] GlobalPlatform. Contactless Services, GlobalPlatform Card Specification v 2.2 - Amendment C v1.0.1, February 2012.

[31] GlobalPlatform. Contactless Services - Amendment C v1.1, April 2013.

[32] GlobalPlatform. GlobalPlatform Card Technology Secure Channel Protocol ’03’ - Amendment D v1.1, January 2011.

[33] GlobalPlatform. Security Upgrade for Card Content Management - Amendment E v1.1, November 2016.

[34] GlobalPlatform. GlobalPlatform Card Secure Channel Protocol ’11’ - Amendment F Version 1.1, September 2017.

[35] GlobalPlatform. GlobalPlatform Technology Executable Load File Upgrade - Version 1.1, March 2018.

[36] GlobalPlatform. GlobalPlatform Technology Secure Element Management Service - Version 1.0, March.

[37] GlobalPlatform. GlobalPlatform common Implementation Configuration - Version 2.0, December 2015.

[38] GSMA. SGP.22 Remote SIM Provisioning (RSP) Technical Specification, version 2.2.1, GSMA Association, December 2018.

[39] GSMA. SGP.22 Remote SIM Provisioning (RSP) Technical Specification, version 2.2.2, GSMA Association, June 2020.

[40] GSMA. SGP.02 Remote Provisioning Architecture for Embedded UICC Technical Specification, version 3.2; 27 June 2017.

[41] GlobalPlatform. GlobalPlatform UICC Configuration v1.0.1, January 2011.

[42] GlobalPlatform. GlobalPlatform UICC Configuration - Contactless Extension Version 1.0, February 2012.

[43] BSI. CSP-API Definition, 5 November 2018.

[44] ETSI. ETSI TS 102 622 v12.1.0 Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI), 10 2014.

[45] Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie - Kryptographische Verfahren: Empfehlungen und Schlüssellängen, 09. Januar 2013, BSI-TR02102.

[46] 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.

[47] FIPS PUB 197: Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, US Department of Commerce/National Institute of Standards and Technology, 26 November 2001.

[48] FIPS PUB 186-4: Digital Signature Standard (DSS), US Department of Commerce/ National Institute of Standards and Technology, 2013.

[49] NIST SP 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques, National Institute of Standards and Technology, December 2001.

[50] NIST SP 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Morris Dworkin, National Institute of Standards and Technology, May 2005.

[51] NIST SP 800-38C: Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality, National Institute of Standards and Technology, May 2005.

[52] National Institute of Standards and USA Technology. NIST Special Publication 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007.

[53] RFC 2104: HMAC: Keyed-Hashing for Message Authentication, Request For Comments, February 1997

[54] Trusted Platform Module Library, Part 1: Architecture, Family “2.0”, Level 00, Revision 01.38, September 2016.

[55] ECDAAFIDO Alliance, Alliance Proposed Standard FIDO ECDAA Algorithm, https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-ecdaa-algorithm-v1.2-ps-20170411.html, April 2017.

10 Legal information

10.1 Definitions

Draft — The document is a draft version only. The content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included herein and shall have no liability for the consequences of use of such information.

10.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors. In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory. Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification. Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products. NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Limiting values — Stress above one or more limiting values (as defined in the Absolute Maximum Ratings System of IEC 60134) will cause permanent damage to the device. Limiting values are stress ratings only and (proper) operation of the device at these or any other conditions above those given in the Recommended operating conditions section (if present) or the Characteristics sections of this document is not warranted. Constant or repeated exposure to limiting values will permanently and irreversibly affect the quality and reliability of the device.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

No offer to sell or license — Nothing in this document may be interpreted or construed as an offer to sell products that is open for acceptance or the grant, conveyance or implication of any license under any copyrights, patents or other industrial or intellectual property rights.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Non-automotive qualified products — Unless this data sheet expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications. In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

Translations — A non-English (translated) version of a document is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — While NXP Semiconductors has implemented advanced security features, all products may be subject to unidentified vulnerabilities. Customers are responsible for the design and operation of their applications and products to reduce the effect of these vulnerabilities on customer's applications and products, and NXP Semiconductors accepts no liability for any vulnerability that is discovered. Customers should implement appropriate design and operating safeguards to minimize the risks associated with their applications and products.

10.3 Trademarks

Notice: All referenced brands, product names, service names and trademarks are the property of their respective owners.

MIFARE — is a trademark of NXP B.V.

DESFire — is a trademark of NXP B.V.

Tables

Figures

Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 17 June 2021
Document identifier: ST-JCOP52R3-02