IDEMIA

MobileID on Dakota IoT -

Public Security Target

Reference: FQR 041467_01

Ed.9

DOCUMENT EVOLUTION

Date	Version issue	Author	Revision
03/11/2025	9	IDEMIA	Public ST for publication

Table of contents

Table of figures

Table of tables

1 Security Target Introduction

1.1 Introduction

This document is the Security Target lite for the MobileID application installed on the IDEMIA Dakota IoT platform. The MobileID application is an IDEMIA Java Card application designed to provide identification, authentication and advanced signature or seal creation functionality for national ID cards, health cards and corporate cards.

The MobileID application can be used to create advanced or qualified signature in the sense of [eIDAS] in its Qualified Signature Creation Device (QSCD) configuration defined in this security target and complies eIDAS v2 specification [TR SIG].

The MobileID can be also used for seal creation according to Qualified Seal Creation Devices as defined in [eIDAS].

Dakota IoT is an IDEMIA Global Platform Java Card solution, which is Common Criteria EAL4+ certified on top of the IDEMIA Starchip SC31 security controller. Note that in this document the SC31 marketing name is for SCE900U IDEMIA IC [IC_CERT].

This ST has been conceived to prepare a Common Criteria evaluation following the "compositional approach" described in [COMP]. This approach consists in starting from a Platform that has been independently certified, and performing an evaluation of the composite product resulting from embedding an Application into it, using some of the results from the evaluation of the Dakota open platform certified by the NSCIB.

This Security Target lite describes:

1. The Target of Evaluation (TOE)
2. The assets to be protected, the threats (T) to be countered by the TOE itself during the usage of the TOE,
3. The organizational security policies (OSP), and the assumptions (A),
4. The security objectives (OT) for the TOE and its environment (OE),
5. The security functional requirements (SFR) for the TOE and its IT environment,
6. The TOE security assurance requirements (SAR), and
7. The TOE Summary specification (TSS).

1.2 ST Reference

Title	MobileID on Dakota IoT – Public Security Target
Reference	041467_01
Version	9
CC Version	CC:2022, Revision 1
Assurance Level	EAL4 augmented with ALC_DVS.2, AVA_VAN.5 and ALC_FLR.3
ITSEF	SGS Brightsight
Certification Body	NSCIB
Author	IDEMIA

Title	MobileID on Dakota IoT – Public Security Target
Protection Profiles	PP SSCD-Part 2 Key Generation [PP-SSCD2], PP SSCD-Part 3 Key Import [PP-SSCD3]

1.3 TOE Reference

TOE Commercial Name	MobileID on Dakota IoT
Applet Code Version (SAAAAR Code)	09AF41
Platform Certificate	[PTF_CERT]
IC Certificate	[IC_CERT]
Guidance Documents	Refer to Table 3 - TOE Guidance under TOE Overview Section

Note:

The "SAAAAR" is product version number within IDEMIA uniquely defined as:

S	IDEMIA Site code	1 byte
AAAA	Article number	4 bytes
R	Software Release number	1 byte

2 Technical Terms, Abbreviation and Associated References

2.1 Technical terms

Term	Definition
Application note	*Optional informative part of the ST containing sensitive supporting information that is considered relevant or useful for the construction, evaluation or use of the TOE.*
Administrator	*User who performs TOE initialization, TOE personalization, or other TOE administrative functions.*
Advanced electronic signature	*An electronic signature which meets the following requirements [DIR]:* *(i) it is uniquely linked to the signatory,* *(ii) it is capable of identifying the signatory,* *(iii) it is created using means that the signatory can maintain under his sole control,* *(iv) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.*
Authentication data	*Information used to verify the claimed identity of a user.*
Authentication	*Authentication defines a procedure that verifies the identity of the communication partner. The most elegant method is based on the use of so called digital signatures.*

Certificate	*Digital signature used as electronic attestation binding signature-verification data to a person confirming the identity of that person as legitimate signer.*
Certificate info	*Information associated with an SCD/SVD pair that may be stored in a secure signature creation device* *NOTE 1: Certificate info is either* - *a signer's public key certificate or,* - *one or more hash values of a signer's public key certificate together with an identifier of the hash function used to compute the hash values.* *NOTE 2: Certificate info may contain information to allow the user to distinguish between several certificates.*
Certificate-generation application (CGA)	*Collection of application components that receive the SVD from the SSCD to generate a certificate obtaining data to be included in the certificate and to create a digital signature of the certificate.*
Certificate revocation list	*A list of revoked certificates issued by a certificate authority.*
Certification service provider (CSP)	*Entity that issues certificates or provides other services related to electronic signatures.*
CLFDB	*Ciphered Load File Data Block* *Defined in Global Platform load encrypted applets. Decryption occurs with a GP symmetric CLFDB key installed in the SSD or ISD.*
Data to be signed (DTBS)	*All of the electronic data to be signed including a user message and signature attributes*
Data to be signed or its unique representation (DTBS/R)	*Data received by a secure signature creation device as input in a single signature creation operation* *NOTE: Examples of DTBS/R are* - *a hash value of the data to be signed (DTBS), or* - *an intermediate hash value of a first part of the DTBS complemented with a remaining part of the DTBS, or* - *the DTBS.*
ECC	*(Elliptic Curve Cryptography) class of procedures providing an attractive alternative for the probably most popular asymmetric procedure, the RSA algorithm.*
eIDAS	*Electronic Identification, Authentication and Trust Services , this is the European regulation.*
Hash function	*A function which forms the fixed-size result (the hash value) from an arbitrary amount of data (which is the input). These functions are used to generate the electronic equivalent of a fingerprint. The significant factor is that it must be impossible to generate two entries which lead to the same hash value (so called collisions) or even to generate a matching message for a defined hash value.*

Integrity	*The test on the integrity of data is carried out by checking messages for changes during the transmission by the receiver. Common test procedures employ Hash functions, MACs (Message Authentication Codes) or – with additional functionality – digital signatures.*
Javacard	*A smart card with a Javacard operation system.*
Legitimate user	*A user of a secure signature creation device who gains possession of it from an SSCD provisioning service provider and who may be authenticated by the SSCD as its signatory.*
MAC	*Message Authentication Code. Algorithm that expands the message by means of a secret key by special redundant pieces of information, which are stored or transmitted together with the message. To prevent an attacker from targeted modification of the attached redundancy requires its protection in a suitable way.*
Notified body	*An organizational entity designated by a member state of the European Union as responsible for accreditation and supervision of the evaluation process for products conforming to [PP-SSCD2], [PP-SSCD5] and for determining admissible algorithms and algorithm parameters.*
Non repudiation	*One of the objectives in the employment of digital signatures. It describes the fact that the sender of a message is prevented from denying the preparation of the message. The problem cannot be simply solved with cryptographic routines, but the entire environment needs to be considered, and respective framework conditions need to be provided by pertinent laws.*
Private key	*Secret key only known to the receiver of a message, which is used in asymmetric ciphers for encryption or generation of digital signatures.*
Pseudo random number	*Many cryptographic mechanisms require random numbers (e.g. in key generation). The problem, however, is that it is difficult to implement true random numbers in software. Therefore, so called pseudo random number generators are used, which then should be initialized with a real random element (the so-called seed).*
Public Key	*Publicly known key in an asymmetric cipher which is used for encryption and verification of digital signatures.*
Public key infrastructure (PKI)	*Combination of hardware and software components, policies, and different procedures used to manage digital certificates.*
Qualified certificate	*Public key certificate that meets the requirements laid down in Annex I and that is provided by a CSP that fulfils the requirements laid down in Annex II (the directive: 2.10) [DIR].*
Qualified electronic signature	*Advanced electronic signature that has been created with an SSCD with a key certified with a qualified certificate ([DIR]: 5.1).*
Random numbers	*Many cryptographic algorithms or protocols require a random element, mostly in form of a random number, which is newly generated in each case. In these cases, the security of the procedure depends in part on the suitability of these random numbers. As the generation of real random numbers within computers still imposes a problem (a source for real random events can in fact only be gained by exact observation of physical events, which is not easy to realize for software), so called pseudo random numbers are used instead.*

Reference authentication data (RAD)	*Data persistently stored by the TOE for authentication of a user as authorised for a particular role.*
Secure messaging	*Secure messaging using encryption and message authentication code.*
Secure signature creation device (SSCD)	*Personalized device that meets the requirements laid down in [DIR], Annex III by being evaluated according to a security target conforming to this PP ([DIR]: 2.5 and 2.6).*
Signatory	*legitimate user of an SSCD associated with it in the certificate of the signature-verification data and who is authorized by the SSCD to operate the signature-creation function.*
Signature attributes	*Additional information that is signed together with a user message.*
Signature creation application (SCA)	*Application complementing an SSCD with a user interface with the purpose to create an electronic signature. Note: A signature creation application is software consisting of a collection of application components configured to:* ▪ *present the data to be signed (DTBS) for review by the signatory,* ▪ *obtain prior to the signature process a decision by the signatory,* ▪ *if the signatory indicates by specific unambiguous input or action its in-tent to sign send a DTBS/R to the TOE,* ▪ *process the electronic signature generated by the SSCD as appropriate, e.g. as attachment to the DTBS.*
Signature creation data (SCD)	*Private cryptographic key stored in the SSCD under exclusive control by the signatory to create an electronic signature.*
Signature creation system (SCS)	*Complete system that creates an electronic signature consisting of an SCA and an SSCD.*
Signature verification data (SVD)	*Public cryptographic key that can be used to verify an electronic signature.*
Signed data object	*The electronic data to which the electronic signature has been attached to or logically associated with as a method of authentication.*
Smart card	*A smart card is a chip card which contains an internal micro controller with CPU, volatile (RAM) and non-volatile (FLASH) memory, i.e. which can carry out its own calculations in contrast to a simple storage card. Sometimes a smart card has a numerical coprocessor (NPU) to execute public key algorithms efficiently. Smart cards have all their functionality comprised on a single chip (in contrast to chip cards, which contain several chips wired to each other). There-fore, such a smart card is ideal for use in cryptography as it is almost impossible to manipulate its internal processes.*

SSCD provisioning service	*Service to prepare and provide an SSCD to a subscriber and to support the signatory with certification of generated keys and administrative functions of the SSCD.*
User	*Entity (human user or external IT entity) outside the TOE that interacts with the TOE.*
User Message	*Data determined by the signatory as the correct input for signing.*
Verification authentication data (VAD)	*Data provided as input to a secure signature creation device for authentication by cognition.*

2.2 Abbreviation

Acronym	Definition
ADF	*Application Dedicated File*
CA	*Certification authority*
CAD	*card acceptance device*
CC	*Common Criteria*
CGA	*Certification generation application*
CPU	*Central Processing Unit*
CSP	*certification service provider*
DPA	*differential power analysis*
DTBS	*Data to be signed*
DTBS/R	*Data to be signed or its unique representation*
EAL	*Evaluation assurance level*
ECC	*Elliptic Curve Cryptography*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
GP	*Global Platform*
HID	*human interface device*
IT	*Information technology*
MAC	*Message Authentication Code*

OSP	*Organizational security policy*
PIN	*Personal Identification Number*
PP	*Protection profile*
PS	*Personalization System*
PUK	*PIN Unblocked Key*
RAD	*Reference authentication data*
RAM	*random access memory*
RNG	*random number generation*
SAR	*Security Assurance Requirements*
SCA	*Signature creation application*
SCD	*Signature creation data*
SCS	*Signature creation system*
SDO	*Security data object*
SF	*security function*
SFP	*Security function policy*
SFR	*Security functional requirement*
SPA	*simple power analysis*
SSCD	*Secure signature creation device*
ST	*Security target*
SVD	*Signature verification data*
TOE	*Target of evaluation*
TSF	*TOE security functionality*
VAD	*Verification authentication data*

2.3 References

Reference	Description
[CC1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, version CC:2022, Revision 1, November 2022.
[CC2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, version CC:2022, Revision 1, November 2022.
[CC3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, version CC:2022, Revision 1, November 2022.
[CC4]	Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities November 2022, CC:2022 Revision 1.
[CC5]	Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements November 2022, CC:2022 Revision 1.
[CEM]	Common Methodology for Information Technology Security Evaluation, Evaluation methodology November 2022 CEM:2022 Revision 1.
[COMP]	Composite product evaluation for smart cards and similar devices, Version 1.5.1, May 2018.
[PP-IC]	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, Registered and Certified by Bundesamt für Sicherheit in der Informations Technik (BSI) under the reference BSI-CC-PP-0084-2014.
[PP-JVC]	Java Card™ System - Open Configuration Protection Profile, version 3.0.5, December 2017, BSI-CC-PP-0099-2017.
[PP-eUICC]	Embedded UICC for Consumer and IOT Devices Protection Profile, GSMA SGP.25 v2.1.
[PP-SSCD2]	Protection profiles for secure signature creation device — Part 2: Device with key Generation, EN 419211-2:2013, CEN/TC 224, BSI-CC-PP-0059-2009-MA-02, Version 2.0.1, June 30 2016.
[PP-SSCD3]	Protection profiles for secure signature creation device – Part3: Device with key import, EN 419211-3:2013, CEN/TC 224, BSI-CC-PP-0075-2012-MA-01, Version 1.0.2, June 30 2016.
[PP-SSCD5]	Protection profiles for secure signature creation device — Part 5: Extension for device with key generation and trusted channel to signature creation application, EN 419211-5:2013, CEN/TC 224, BSI-CC-PP-0072-2012-MA-01, Version 1.0.1, June 30 2016.

Reference	Description
[ST-PL]	Public Security Target - DaKota IoT v1.1 Phase 2 on SCE900U FQR 110 A41B Ed 2.
[PTF_CERT]	NSCIB-CC-2500034-01.
[IC_CERT]	ANSSI-CC-2024/19.
[AGD_PRE]	Mobile Id Applet Perso Guide FQR 110 A435 Ed 2.3.
[AGD_OPE]	Mobile Id Applet V1.0 Operational User Guidance (AGD_OPE) FQR 110 A432 Ed 1.2
[CICC]	ISO/IEC 14443 Identification cards -- Contactless integrated circuit cards -- Proximity cards, 2008-11.
[ICC]	ISO/IEC 7816: Identification cards — Integrated circuit cards, Version Second Edition, 2008.
[14890]	CEN/EN 14890:2013 Application Interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional Services.
[AIS20]	Bundesamt fuer Sicherheit in der Informationstechnik. Anwendungshinweise und Interpretationen zum Schema, AIS 20: Funktionalitaetsklassen und Evaluationsmethodologie fuer deterministische Zufallszahlengeneratoren, Version 2.1, 2.12.2011.
[TR_SIG]	Technical report Signature creation and administration for eIDAS token Part 1: Functional Specification version 1.0 2015/07/21.
[DIR]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures.
[EU-REG-910/2014]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[EU-IMP-2016-650]	COMMISSION IMPLEMENTING DECISION (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market.
[EU-IMP-2024-1183]	REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework - 30.4.2024.
[JCRE]	Published by Oracle. Java Card 3 Platform, Runtime Environment Specification, Classic Edition, Version 3.0.5, May 2015.

Reference	Description
[JCAPI]	Published by Oracle. Java Card 3 Platform, Application Programming Interface, Classic Edition, Version 3.0.5. May 2015.
[GP]	GlobalPlatform Card Specification 2.3.1, GlobalPlatform Inc., March 2018.
[JCVM]	Published by Oracle. Java Card 3 Platform, Virtual Machine Specification, Classic Edition, Version 3.0.5, May 2015.
[Minidriver]	Windows Smart Card Minidriver Specification - V.ersion 7.06 – July 1, 2009.
[TR03110]	[TR03110-2] and [TR03110-3].
[TR03110-3]	BSI: TR-03110-3: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token. Part 3 - Common Specifications, Version 2.21, 21 December 2016.
[SCP03]	Global Platform Card Technology, Secure Channel Protocol '03' – Card Specification v2.2 – Amendment D – Version 1.1.1 – July 2014.
[ISO_15946]	[ISO_15946-2] and [ISO_15946-3].
[ISO_15946-2]	ISO/IEC15946-2. Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures, 2002.
[ISO_15946-3]	ISO/IEC 15946: Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment, 2002.
[eIDAS]	REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[SEC1]	Standards for Efficient Cryptography SEC 1: Elliptic Curve Cryptography May 21, 2009 Version 2.0.
[SGP_02]	GSMA SGP.02 - Remote Provisioning Architecture for Embedded UICC Technical Specification v4.1.
[TS_102225]	SCP80 - ETSI TS 102 225 - Secured packet structure for UICC based applications, version 12.0.0, release 12.
[AIS]	A Proposal for Functionality Classes for Random Number Generators version 2.0, September 18th, 2011.

3 TOE Overview

The TOE comprises of the IDEMIA MobileID signature application installed on top of the eUICC IDEMIA Dakota IoT Global Platform Java Card and Telecom operating system based on the IDEMIA SC31 security controller.

The MobileID application is an IDEMIA specific Java Card implementation designed to provide functionality for identification, authentication and advanced digital signature creation for mobile phone , national ID cards, health cards or corporate cards.

The Dakota IoT platform has been Common Criteria EAL4+ certified on top of the IDEMIA SC31 security controller [See ST-PL]. The IDEMIA SC31 is a Common Critieria EAL5+ certificed security controller.

In its Qualified Signature Creation Device (QSCD) configuration defined in this security target, MobileID application instances can create advanced (qualified) digital signatures in the sense of [eIDAS].

In its Qualified Seal Creation Devices (QSeal) configuration MobileID application instances can create seal in the sense of [eIDAS]. At personalization QSCD or QSeal can be determined.

The MobileID application complies to the eIDAS v2 specification [TR03110] and therefore supports authentication protocols for symmetric secure messaging ciphers AES128, AES192, AES256. This feature is provided by the platform and used for secure messaging.

The TOE addressed by this ST is a qualified electronic signature creation device QSCD/SSCD according to European Regulation eIDAS v2 [EU-REG-910/2014], [EU-IMP-2024-1183] and implementing act [EU-IMP-2016-650] with functionality covered in (a combination of) the following SSCD protection profiles:

1) SSCD Part 2: that performs the generation of signature keys in the device [PP-SSCD2],
2) SSCD Part 3: that performs the import of the signature keys generated in a trusted manner outside the device [PP-SSCD3],

The objective from the SSCD Part 5, OT.TOE_TC_DTBS_Imp is added in this security target. It allows the detection of any alteration of DTBS/R received and forbid signature on altered DTBS.

Dedicated SFRs are added to answer to the security objective added: FTP_ITC.1/DTBS and by FDP_UIT.1/DTBS.

Note
The added security objectives for the operational environment don't mitigate any threats of [PP-SSCD2], [PP-SSCD3], and don't fulfil any OSPs meant to be addressed by security objectives for the TOE in [PP-SSCD2], [PP-SSCD3. The objectives and SFRs related to the functionality are only valid in case the additional functionalities are configured for the TOE. The added objective from [PP-SSCD5] don't mitigate any threat of the PPs. It adds protection on the exchanges between SCA and the TOE.

4 TOE Description

4.1 TOE Type

The TOE is a combination of hardware and software configured to securely create, use and manage signature creation data.

The TOE consists of:

- The chip's circuitry and the IC dedicated software forming the Chip Platform (Hardware Platform).
- The IC embedded Dakota IoT Global Platform Java Card operating system software consisting of
    - Java Card virtual machine, ensuring language-level security;
    - Java Card runtime environment, providing additional security features for Java card technology enabled devices;
    - Java card API, providing access to card's resources for the Applet;
    - Global Platform Card Manager, responsible for management of Applets on the card;
    - GSMA framework: an eUICC Operating System with telecom framework and profile management.
- MobileID Applet for signature generation.
- TOE Guidance documentation for the MobileID application and the Dakota platform as specified in Table 2.
- The Global Platform Key Set (for TOE preparation by the Personalization Agent).

The MobileID application provides e-Services based on Java Card. MobileID is designed to be compliant with the eIDAS v2 specification [TR03110]. It provides the following services:

1) QSCD/SSCD containing sensitive private keys needed for generating qualified electronic signatures on behalf of the Card Holder as well as for user authentication and identification. The MobileID application is intended to be used in the context of official and commercial services, where an electronic digital signature of the Card Holder is required and is to be certified according to [PP-SSCD2] and [PP-SSCD3].

4.1.1 Physical Scope

The TOE is physically made up of several components hardware and software. Once constructed, the TOE is a bare microchip with its external interfaces for communication. The physical form factor (chip module or antenna inlay, etc.) into which the microchip is mounted is not part of the target of evaluation, because it does not alter nor modify any security functions of the TOE. The TOE is provided with MobileID applet to be personalized.
The TOE may be used on several physical form factors: modules within an inlay, or eCover; in a contact, contactless or dual plastic card.

The physical form factor of the TOE and its physical interfaces are depicted in Figure below. The cryptographic boundary of the module is the surface and edges of the die and associated bond pads, shown as circles in the following figure.

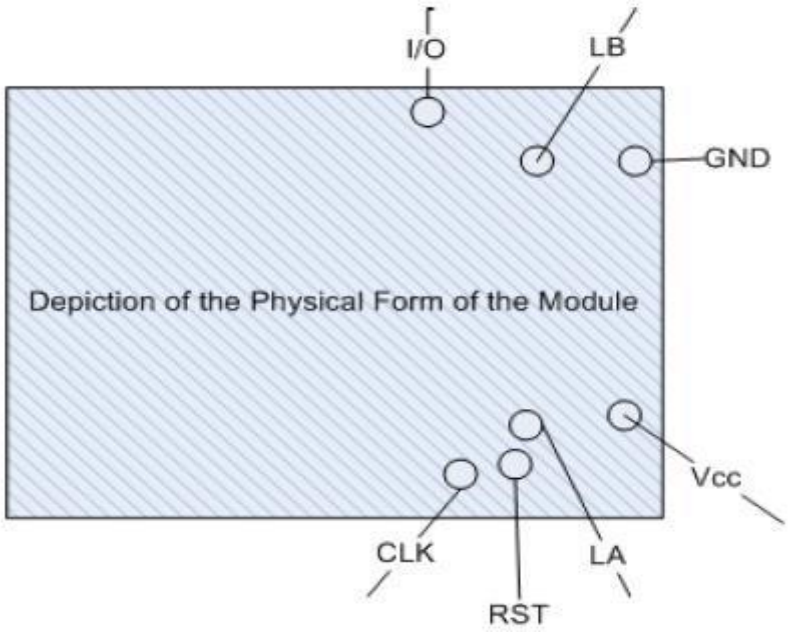

Figure 1: TOE's Physical form factor and interfaces

The contactless ports of the module require connection to an antenna. The module relies on [ISO7816] and [ISO14443] card readers and antenna connections as input/output devices.

Port	Description	Logical Interface Type
VCC, GND	ISO 7816: Supply voltage	Power (not available in contactless-only configurations)
RST	ISO 7816:Reset	Control in (not available in contactless-only configurations)
CLK	ISO 7816: Clock	Control in (not available in contactless-only configurations)
I/O	ISO 7816: Input/ Output	Control in, Data in, Data out, Status out (not available in contactless-only configurations)
LA, LB	ISO 14443: Antenna	Power, Control in, Data in, Data out, Status out (Not available in Contact-only configurations)

Table 1 Ports and Interfaces

The following guidance documents will be provided for the TOE:

Description	Audience	Form Factor of Delivery
[AGD_PRE]	Personalizer of the TOE	Electronic Version
[AGD_OPE]	End User of the TOE	Electronic Version
Platform Guidance: Platform related guidance documents are mentioned in **[ST-PL]**.	Platform users	Electronic Version

Table 2 TOE Guidance

An ST Lite version of this Security Target will also be provided along with above mentioned documents. All the above-mentioned guidance documents will be delivered by mail in a .pgp encrypted and signed format.

Form factor and Delivery Preparation:

1. In accordance with the software development process of IDEMIA, upon completion of development activities, particular applet will be uploaded into PS in CAP file format.
2. During Release for Sample as project milestone, status of the applet in PS will be changed into "Pilot version" to be used further for manufacturing samples.
3. During Software Delivery Review as the final R&D project milestone, status of the applet in PS will be changed into "Industrial release" to be used further for mass production.

Refer Life Cycle chapter of this ST for more details regarding TOE delivery as per different options.

4.1.2 Logical Scope

The Mobile ID application on Dakota IoT platform is in an integrated circuit chip with:

- The Idemia SC31 chip
- An Idemia Dakota Operating system providing:
  - Java Card interfaces, as specified in [JCAPI]
  - GSMA interfaces for targeted applications needs
  - A card manager application compliant with the Global Platform v2.3.1 specifications [GP] standard.

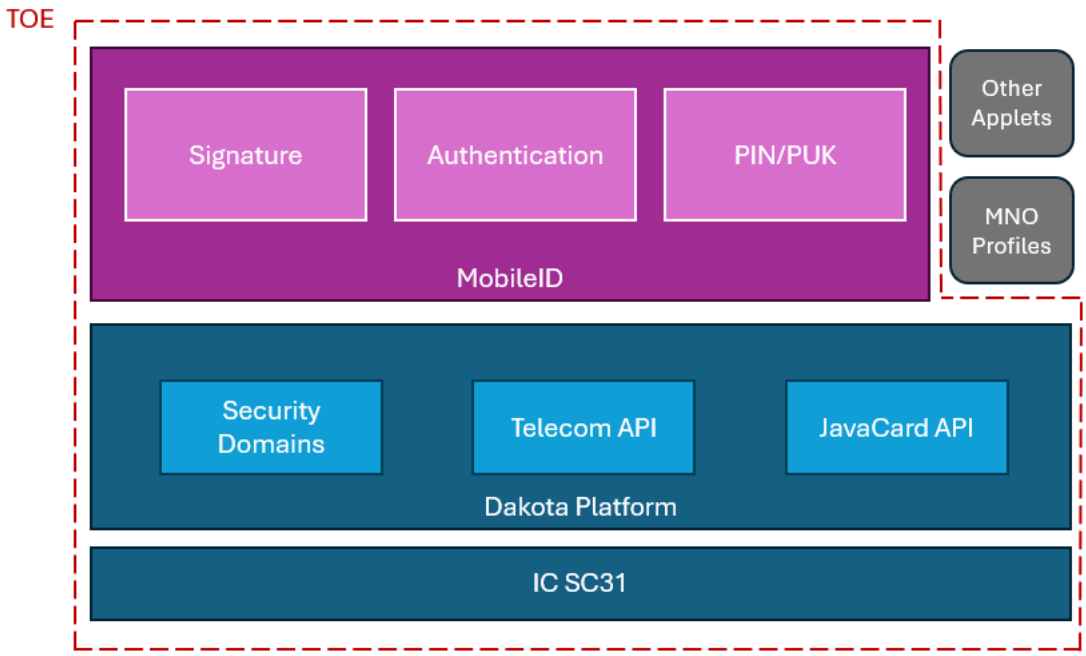

Figure 2: TOE Logical scope

4.2 Required non-TOE hardware/software/firmware

The TOE is a Qualified Signature Creation Device. The TOE relies on an eUICC JavaCard Open Platform and requires a mobile handset connectivity with the Mobile Network Operator.

Before the applet loading the TOE uses a bytecode verifier as required by platform.

Any applet installed on the platform (not only MobileID) shall pass the bytecode verification.

To be powered up and to be able to communicate, the TOE needs a reader, terminal or mobile handset.

The TOE does not need any additional hardware/software/firmware to ensure its security.

4.3 TOE Usage and Major Security Features

The TOE allows performing authentication and signature to be used in communicating with the mobile phone. Mobile-ID is an e-identity available on the end-user's phone, for secure and convenient authentication and electronic signing.
The scope of [PP-SSCD2], [PP-SSCD3] and subset of [PP-SSCD5] is extended in several ways:

- A super Administrator (TOE_Administrator) has special rights to administrate the signature creation function and the type of cryptographic mechanisms to use.
- SCD/SVD pairs and other cryptographic objects may be generated after issuance at any time, and in particular, they may be updated during the TOE life cycle.
- eServices features are added, enabling the cardholder to perform C/S authentication.
- A complete access control over objects is ensured, whatever their type is: file or cryptographic objects (PIN, keys,…), ensuring it is not possible to bypass the access rules.
- Personalization phase including:
  - authentication protocol;

- access control;
- encryption mechanism involved in key loading;
- initialization of the data structure;
- data loading;
- locks management;
- phase switching.

- All authentication protocols (symmetric and asymmetric), and secure messaging type (AES128/192/256) provided by the platform;
- All supported digital signature algorithm;
- Authentication of the TOE using symmetric and asymmetric cryptography;
- All PIN management operations available after delivery point;
- Certificate management.

The TOE may be used for various use cases requiring qualified signature:

- Electronic signature application;
- Electronic health card;
- Electronic services cards.

Depending on the use case and or the ability of the underlying java card open platform, the TOE may be used:

- in contact mode (T=0 and/or T=1 protocol);
- in contactless protocol (T=CL).

Since the TOE claims compliancy to protection profiles from 419 211-2 and EN 419 211-3 and is partly based on EN 419-5 (Signature Protection Profiles [PP-SSCD2], [PP-SSCD3] with some additions from the [PP-SSCD5]), the TOE can (depending on the desired card profile/issuer policy) be used in the following QSCD/SSCD configurations:

- **SSCD Config#1** claiming compliancy to CEN/EN 419 211-2/3/ ([PP-SSCD2], [PP-SSCD3]. The configuration implements additional part for the establishment of a trusted channel between the TOE and the SCA from [PP-SSCD5]).
- **SSCD Config#2** claiming compliancy to CEN/EN 419 211-2/3 ([PP-SSCD2], [PP-SSCD3]). This configuration does not support the trusted channel between the TOE and the SCA.

The TOE provides security features presented in the next paragraphs.

4.3.1 Personalization

The personalization of Mobile Id Applet is typically performed as follows:

- Select the applet instance
- Perform GP Authentication
- Load configuration data
- Load the EC domain parameters
- Load or generate up to 4 EC keys
- Load up to 4 PINs
- Load the PUK
- Load the Text/Prompt Strings for all languages
- Switch to PERSONALIZED state

The state NOT INSTALLED and LOCKED are controlled by the Card Manager. The transitions to/from these states are described in [GP] and are out of the scope of this document.

4.3.2 Key Management

The applet manages 4 EC key pairs (consisting of public and private keys) using the same set of EC-256 domain parameters. The domain parameters are configured in SELECTABLE state. The values of each of the 4 EC key pairs may optionally be loaded by the personalization agent or generated on card in SELECTABLE state. It is possible to create new or overwrite each of these key pairs by instructing the applet to generate new key pairs in PERSONALIZED state.

During creation, each of these keys are assigned with specific usage such as authentication or signing.

4.3.3 PIN and PUK Management

The applet manages 4 PINs and a PUK. The attributes of each of these PIN/PUK, such as minimum and maximum length and the retry limit, are loaded in SELECTABLE state. Initial values of these PIN/PUK are also initialized in SELECTABLE state. Each PIN is used to protect the usage of one of the EC key pairs.

In PERSONALIZED state, it is possible to change and unblock the PIN/PUK.

4.3.4 Registration

Registration consists in loading/generating an EC key pair and associating it with a PIN and a role (authentication or signing). Once registered, the key is ready to be used for authentication or signature generation, depending on its role. Registration is done either in SELECTABLE or PERSONALIZED state.

4.3.5 Authentication and Signing

During authentication and signing operations, the applet computes a digital signature from input hashed data and other parameters, using the selected EC private key, after a successful verification of its associated PIN. The signature is returned as part of the response data.

The TOE intended usage is to be used as a "Qualified Signature Creation Device" with key generation and/or key import, with respect to the [EU-IMP-2024-1183].
The TOE allows to

- perform basic, advanced and qualified signatures;
- authenticate the cardholder based on a PIN verification;
- authenticate one (or several) administrator(s) of the TOE, that may have special rights to administrate the SCD and SVD (generation, import), using either symmetric and/or asymmetric mechanisms, or PIN verification;
- establish trusted channel, protected in integrity and confidentiality, with Trusted IT entities such as a SCA or a CSP. It may be realized by means of symmetric and/or asymmetric mechanisms.

4.3.6 Authentication mechanisms

This feature realizes the following authentication mechanisms:

- User authentication (PIN)
- External authentication (symmetric and asymmetric role authentication)
- Secure messaging (symmetric and asymmetric device authentication)
- GP authentication in phase 6 (personalizer) and 7 (TOE admin)
- combined device/role authentication

It also ensures that only authenticated terminals can get access to the user data stored on the TOE.

4.3.7 Cryptographic operations

This feature performs high level cryptographic operations (key generation, symmetric and asymmetric encryption and decryption, signature creation, destruction of cryptographic keys and random number generation). The TOE uses implementation based on the Security Functionalities provided by the platform.

4.3.8 Trusted Channel function

This feature realizes a secure communication channel to verify authenticity and integrity as well as securing confidentiality of user data between the TOE and other devices connected. The TOE provides:

- Secure messaging with external applications as CGA and SCA
- GP secure messaging in phase 6
- AES128, AES192 and AES256 for encryption/decryption and MAC generation/verification

This feature is provided by the platform and used for secure messaging.

4.3.9 Access Control function

This feature manages the access to objects (files, directories, data and secrets) stored in the MobileID file system. It ensures secure management of secrets such as cryptographic keys. Access control is enforced by the APDU or SMS methods as specified in the interface defined in the functional specification.

4.3.10 Data Storage function

This feature manages the storage of manufacturing data and personalization data. This covers also the secure storage of SCD/SVD and RAD.

4.3.11 Integrity function

This feature monitors the integrity of sensitive user data and the integrity of the DTBS/R.

4.3.12 Electronic Services

The TOE supports several electronic services:

- C/S authentication: this feature enables to authenticate the TOE to an external entity.
- Digital signature: this feature enables the cardholder to electronically signs documents. The signature may be either advanced or qualified (compliant with [PP-SSCD2] and [PP-SSCD3]).

4.3.13 Keys and PINs management

The TOE handles as well cryptographic data objects, such as keys (for digital signature, authentication, encryption etc.) and PINs.
The TOE enables to create, update and use PINs as detailed in [AGD_OPE].
For keys, the TOE enables to create, import, generate and erase keys as detailed in [AGD_OPE].

4.3.14 Features from the Platform

This contains all security functionalities provided by the certified platform (IC and Java Card operation system):

- Protection against malfunctions that are caused by exposure to operating conditions that may cause a malfunction. This includes hardware resets and operation outside the specified norms.

- Protection against tampering and the stored assets can not be retrieved or altered by physical manipulation
- Protection against physical attack and perform self tests as described in [ST-PL].
- Security domains are supported by the Java Card platform.
- Cryptographic operations: Signature generation, signature creation and secure messaging, symmetric and asymmetric encryption and decryption and key generation.

5 Life Cycle

The TOE life cycle in the following figure distinguishes stages for development, production, preparation and operational use in accordance with the standard smart card life cycle [PP-IC] and [PP-eUICC].

Phase PP0084	Phase eUICC	eUICC Phase name	Applet Phase	Actors
1 and 2	a	*eUICC platform development*: development of IC and Embedded software	*MobileID and any other application is developed in these stages*	IC: IDEMIA Starchip Embedded Software: OS and MobileID IDEMIA R&D (Jakarta, Courbevoie and Pessac)
3 and 4	b	*eUICC platform storage, platform pre-personalization, tests* – Security IC manufacturing and packaging	*Applets is not involved in this stage*	IC IDEMIA Starchip Packaging: IDEMIA or another agent IC can be sent by IDEMIA or UTAC USG1 or UMC Fab 12I (see IC certificate).
5	c	*eUICC platform storage, pre-personalization, test integration of Platform Software*. Platform Loading (using IC Package 1) Integration of Platform Software, platform pre-perso data and applications.	*With the OS code, applets can be loaded in this stage.* *Prepersonalisation of the platform is done in this phase.*	In audited IDEMIA plants (Vitré, Shenzhen and Noida). OS on IC and MobileID same actors: Audited IDEMIA plants (Vitré, Shenzhen and Noida-P)
6	d1	*eUICC Personalization*	*in phase d1, the platform is personalized.* *Applets can be loaded in this phase.*	In audited IDEMIA plants (Vitré, Shenzhen and Noida).
	d2	*MobileID personalisation*	*The TOE is auto protected in this step its delivered in d2 for MobileID Personalization*	The personalization of MobileID can only be done at any site (see details hereafter).
7	e	*Operational Usage*	*Operational Usage*	The end user

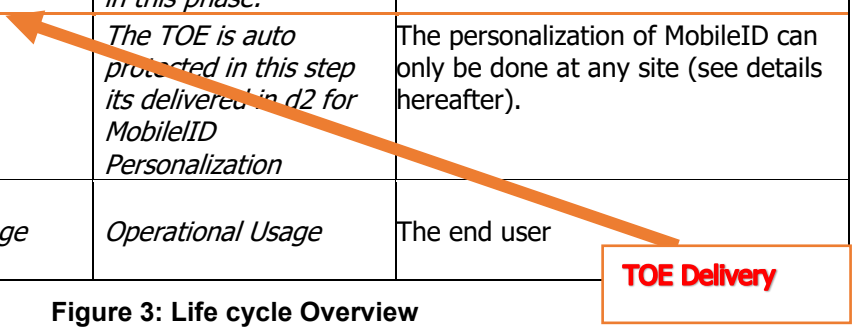

Figure 3: Life cycle Overview

The delivery of the TOE is done after phase 6-d1. Expressed in the red line in figure 3.

This life cycle is completely described in OS platform |ST-PL]. It distinguished the [PP-IC] and the [PP-eUICC]. Note that the [PP-JVC] is also based on [PP-IC] life cycle.

5.1.1 Development Environment

In this environment, the following two phases take place:

- Phase 1: IC Embedded Software Development (Java Card Open Platform components and MobileID Applet)
- Phase 2: IC Development

The IC Embedded Software Developer is in charge of the specification and the development of the software (Java Card Open Platform). This is explained in the ST [ST-PL].

The IC Developer designs the IC, develops the IC dedicated software and provides information, software or tools to the IC embedded software developer.
The hardware Product life cycle covers Security IC development which is described in the IC ST identification (see corresponding ST Lite).
Phase 1 concerns also the development of the applet based on the platform guide, see referenced guide in [ST-PL].
Roles, actors and coverage for this environment of the product life cycle are listed in the table below:

Role	Actor	Covered by
MobileID Applet Developer	IDEMIA	ALC
Embedded Software Developer (Java Card Open Platform)	IDEMIA	ALC
IC Developer	IDEMIA	ALC

5.1.2 Phase b: Security IC Manufacturing and packaging

The Phase b of the Composite Product life cycle covers the IC production Phase 5: Composite Product Integration where the IC is directly delivered without the OS.

5.1.3 Applet loading and delivery

The applet with the guidance is available only at IDEMIA audit sites, no external entity can load the applet. It is stored at IDEMIA system. 2 options for the loading:

- The applet can be loaded with the OS code at phase 5 using the process defined in the [PTF_CERT].
- The applet can be loaded encrypted and decrypted by the platform at phase 5 or phase 6 d1.

Audited IDEMIA Production Sites are Vitré, Shenzhen and Noida-P.

Once the applet is loaded, its auto protected and delivered. The details on TOE delivery methods are provided in **[AGD_PRE].**

The delivery of the TOE for MobileID personalisation is done after the loading of the MobileID applet, after d1.

5.1.4 Personalization

After loading, the TOE is self-protected as it requires the authentication of the personalization agent prior to any operation.

The personalization of MobileID can be done anywhere as functionalities are in the scope of this evaluation.
This phase consists of:

1) SSCD MobileID Applet instance creation of MF for the loaded configuration according to [AGD_PRE].
2) MobileID Personalization according to [AGD_PRE].
3) Post- Personalization steps managed by the OS including: ISD life-cycle management.

Details on personalization is provided in **[AGD_PRE].**

5.1.5 Operational Environment

The TOE in this phase is under the control of the User the Signatory and the Administrator.
This phase is covered by [AGD_OPE] and the platform guidance as listed in the [ST-PL].

6 Conformance Claims

6.1 CC Conformance

This Security Target claims conformance to the following documents:

- [CC1],
- [CC2],
- [CC3],
- [CC4],
- [CC5].

Conformance to CC is claimed as follows:

- Part 1,Part 2: conformant

  All the security requirements have been drawn from the catalogue of requirements in [CC2].
- Part 3: conformant, compliant to EAL4 augmented with
  - ALC_DVS.2 (Sufficiency of security measures)
  - AVA_VAN.5 (Advanced methodical vulnerability analysis)
  - ALC_FLR.3 (flaw remediation)

The TOE also includes:

- Dakota IoT Platform.
- IDEMIA IC.

6.2 PP Claims

This security target claims strict conformance to the following PPs:

- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 2: Device with key generation" [PP-SSCD2].
- "Common Criteria Protection Profile for Secure Signature Creation Device – Part 3: Device with key import" [PP-SSCD3].

6.3 Conformance Rationale

Note that SFRs from all signature PPs are adapted to CC:2022 by deprecating FCS_CKM.4 (replaced by FCS_CKM.6): it concerns FCS_CKM.6/CM-SCP. On the same way none extended SFRs are considered as extended SFRs in CC3.1 have been integrated in CC:2022 and Dependences are adapted to CC:2022. Also FPT_TST wording is adapted to CC:2022

This ST claims strict conformance to the above mentioned PPs [PP-SSCD2], [PP-SSCD3]. A detailed justification is given in the following:

1) The SPD of this ST contains the security problem definition [PP-SSCD2], [PP-SSCD3]. The SPD for this ST is described by the same threats, organisational security policies and assumptions as for the TOE in the PPs.

2) The security objectives for the TOE in this ST include all the security objectives for the TOE of the core PPs [PP-SSCD2] and [PP-SSCD3].

3) The assumptions in this ST include A.CSP from [PP-SSCD3]. This assumption doesn't mitigate any threat and doesn't fulfil any OSP meant to be addressed by security objectives for the TOE in the other PPs.

4) The security objectives for the operational environment in this ST include all security objectives for the operational environment of the core PPs [PP-SSCD2] and [PP-SSCD3]

   This ST adapts OE.DTBS_Protect to the support provided by the TOE by new security functionality (cf. OT.TOE_TC_DTBS_Imp) provided by the TOE and changes them into an objective on the TOE ([PP-SSCD5] for details) in config#1.

   OE.DTBS_Protect for SSCD config#2 is added.
   The OE.HID_VAD and OE.SSCD_Prov_Service are for the config#1 and config#2.

5) The SFRs specified in this ST includes all security functional requirements (SFRs) specified in the core PPs [PP-SSCD2] and [PP-SSCD3]. Additional SFRs address:
   a. trusted channel between the TOE and the SCA from [PP-SSCD5]: FDP_UIT.1/DTBS and FTP_ITC.1/DTBS for config#1 and refinement of the SFR SFR FIA_UAU.1 for the establishment of the trusted channel to send the DTBS according.

   FPT_EMS.1 used as extended SFRs in PPs are now defined according [CC2] definitions without loss of information.

6) FMT_MTD.1/Unblock has been added to restrict RAD management and FMT_MTD.1/TOE_State has been added to manage state of the TOE life cycle.

7) The security assurance requirements (SARs) are originally taken from SARs of part 3 [CC3] according to the package conformance EAL 4 augmented with ALC_DVS.2, ALC_FLR.3 and AVA_VAN.5 (the Evaluation Assurance Level EAL4+ of the current ST exceeds with ALC_DVS.2 and FLR.3 the EAL4+ defined by [PP-SSCD2], [PP-SSCD3]).

8) Additional Threats have been added to the TOE:
   - T.Authentication_Replay to cover the threats when an attacker retrieves an authentication cryptogram.

9) To ensure the robustness of eServices key, OT.TOE_AuthKey_Unique is added.

10) To respond to the T.Authentication_Replay an additional Security Objectives has been added: OT.Authentication_Secure and OT.TOE_AuthKey_Unique.

11) To management the life cycle of TOE, OT.Lifecycle_Management has been added.

This security target is compliant with the SPD of [PP-SSCD2][PP-SSCD3] as shown in the following table. The additions are expressed in a dedicated column.

TOE SPDs	**PP SSCD2**	**PP SSCD3**	**Additions**	**Included**
Assumptions				
A.CGA	×	×		×
A.SCA	×	×		×
A.CSP		x		x
Threats				
T.SCD_Divulg	x	x		×
T.SCD_Derive	×	x		×
T.Hack_Phys	×	x		×
T.SVD_Forgery	×	x		×
T.SigF_Misuse	×	x		×
T.DTBS_Forgery	×	x		×
T.Sig_Forgery	×	x		×
T.Authentication_Replay			x	x
P.CSP_QCert	×	x		×
P.QSign	×	x		×
P.Sigy_SSCD	×	x		×
P.Sig_Non-Repud	×	x		×

Table 3 PP SPDs vs. ST

This security target is compliant with the security objectives of [PP-SSCD2], [PP-SSCD3] as shown in the following table, additions to the PPs are expressed in a separate column.

TOE Objectives	PP SSCD2	PP SSCD3	Additions	Included
OT.Lifecycle_Security	x	x		×
OT.SCD/SVD_Auth_Gen	x			×
OT.SCD_Unique	x			×
OT.SCD_SVD_Corresp	x			×
OT.SCD_Secrecy	x	x		×
OT.Sig_Secure	x	x		×
OT.Sigy_SigF	x	x		×
OT.DTBS_Integrity_TOE	x	x		×
OT.TOE_TC_DTBS_Imp			x	x
OT.EMSEC_Design	x	x		×
OT.Tamper_ID	x	x		×
OT.Tamper_Resistance	x	x		×
OT.SCD_Auth_Imp		x		x
OT.Lifecycle_Management			x	x
OT.TOE_AuthKey_Unique			x	x
OT.Authentication_Secure			x	x

	Objectives for the Operational Environment			
	PP SSCD2	**PP SSCD3**	**additions**	**Included**
OE.SVD_Auth	×	×		×
OE.CGA_QCert	×	×		×
OE.SSCD_Prov_Service	×	×		×
OE.SCD/SVD_Auth_Gen		×		×
OE.SCD_Unique		×		×
OE.SCD_SVD_Corresp		×		×
OE.SCD_Secrecy		x		×
OE.HID_VAD	×	×		×
OE.DTBS_Intend	×	×		×
OE.DTBS_Protect	×	×		×
OE.Signatory	×	×		×
OE.SCA_TC_DTBS_Exp			x	x

Table 4 PP Security Objectives vs. ST

This security target is compliant with the security functional requirements of [PP-SSCD2], [PP-SSCD3] as shown in the following table, additions to the PPs are expressed in a separate column.

TOE SFRs	PP SSCD2	PP SSCD3	Additions	Included
FCS_CKM.1	×			×
FCS_CKM.4→FCS_CKM.6	×	×		×
FCS_COP.1	×	×		×
FDP_ACC.1/SCD/SVD_Generation	×			×
FDP_ACF.1/SCD/SVD_Generation	×			×
FDP_ACC.1/SVD_Transfer	×			×
FDP_ACF.1/SVD_Transfer	×			×
FDP_ACC.1/Signature_Creation	×	×		×
FDP_ACF.1/Signature_Creation	×	×		×
FDP_ACC.1/SCD_Import		×		×
FDP_ACF.1/SCD_Import		×		×
FDP_RIP.1	×	×		×
FDP_SDI.2/Persistent	×	×		×
FDP_SDI.2/DTBS	×	×	x	×
FIA_UID.1	×	×		×
FIA_UAU.1	×	×		×
FIA_AFL.1	×	×		×
FMT_SMR.1	×	×		×
FMT_SMF.1	×	×		×
FMT_MOF.1	×	×		×
FMT_MSA.1/Admin	×	×		×
FMT_MSA.1/Signatory	×	×		×
FMT_MSA.2	×	×		×
FMT_MSA.3	×	×		×
FMT_MSA.4	×	×		×

TOE SFRs	PP SSCD2	PP SSCD3	Additions	Included
FMT_MTD.1/Admin	×	×		×
FMT_MTD.1/Signatory	×	×		×
FPT_EMS.1	×	×		×
FPT_FLS.1	×	×		×
FPT_PHP.1	×	×		×
FPT_PHP.3	×	×		×
FPT_TST.1	×	×		×
FDP_UIT.1/DTBS			x	
FTP_ITC.1/DTBS			x	x
FDP_ITC.1/SCD		×		×
FDP_UCT.1/SCD		×		×
FTP_ITC.1/SCD		×		×
FCS_RNG.1			x	×
FMT_MTD.1/Unblock			x	×
FMT_MTD.1/TOE_State			x	×

Table 5 PP SFRs vs. ST

7 Security Problem Definition

7.1 Assets

7.1.1 Primary Assets drawn from the protection profiles

Following primary assets are protected by the TOE as listed below:

D.SCD

Signature Creation Data

Private key used to perform an electronic signature operation. The confidentiality, integrity and signatory's sole control over the use of the SCD must be maintained.

D.SVD

Signature Verification Data

Public key linked to the SCD and used to perform electronic signature verification. The integrity of the SVD when it is exported must be maintained.

D.DTBS/R

Data to be signed or its unique Representation

Set of data, or its representation, which the signatory intends to sign. Their integrity and the unforgeability of the link to the signatory provided by the electronic signature must be maintained.

7.1.2 Additional Assets : TSF Data

1. **Keys:** a. Private or secret keys used to authenticate an external user or entity, or to perform eServices. Their integrity and confidentiality must be maintained

   b. public key used to perform eServices. Their integrity must be maintained.

2. **PIN/PUK:** The applet manages 4 PINs and a PUK (Personal Unlocking Key Code). Each PIN is used to protect the usage of one of the EC key pairs used for authentication or signature.

3. **Session keys**: Keys computed for secure messaging and used to ensure confidentiality and integrity of data.

7.2 Users / Subjects

7.2.1 Subjects drawn from the protection profiles

S.User

End user of the TOE who can be identified as administrator or signatory. The subject S.User may act as S.Admin in the role R.Admin or as S.Sigy in the role R.Sigy.

S.Admin

User who is in charge to perform the TOE initialization, TOE personalization or other TOE administrative functions. The subject S.Admin is acting in the role R.Admin for this user after successful authentication as administrator.

S.Signatory

User who hold the TOE and use it on their own behalf or on behalf of the natural or legal person or entity they represent. The subject S.Sigy is acting in the role R.Sigy for this user after successful authentication as signatory.

7.2.2 Threat agents

S.Attacker

Human or process acting on their behalf located outside the TOE. The main goal of the attacker is to access the SCD or to falsify the electronic signature. The attacker has got a high attack potential and knows no secret.

7.3 Threats

7.3.1 Threats drawn from the protection profiles

T.SCD_Divulg

Storing, copying and releasing of the signature creation data

An attacker stores or copies the SCD outside the TOE. An attacker can obtain the SCD during generation, storage and use for signature creation in the TOE.

T.SCD_Derive

Derive the signature creation data

An attacker derives the SCD from publicly known data, such as SVD corresponding to the SCD or signatures created by means of the SCD or any other data exported outside the TOE, which is a threat against the secrecy of the SCD.

T.Hack_Phys

Physical attacks through the TOE interfaces

An attacker interacts physically with the TOE to exploit vulnerabilities, resulting in arbitrary security compromises. This threat is directed against SCD, SVD and DTBS.

T.SVD_Forgery

Forgery of the signature verification data

An attacker forges the SVD presented by the CSP to the CGA. This results in loss of SVD integrity in the certificate of the signatory.

T.SigF_Misuse

Misuse of the signature creation function of the TOE

An attacker misuses the signature creation function of the TOE to create SDO for data the signatory has not decided to sign. The TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

T.DTBS_Forgery

Forgery of the DTBS/R

An attacker modifies the DTBS/R sent by the SCA. Thus the DTBS/R used by the TOE for signing does not match the DTBS the signatory intended to sign.

T.Sig_Forgery

Forgery of the electronic signature

An attacker forges a signed data object, maybe using an electronic signature which has been created by the TOE, and the violation of the integrity of the signed data object is not detectable by the signatory or by third parties. The signature created by the TOE is subject to deliberate attacks by experts possessing a high attack potential with advanced knowledge of security principles and concepts employed by the TOE.

7.3.2 Added Threats

T.Authentication_Replay

An attacker retrieves by observation authentication data used by a third party during an authentication sequence. The attacker tries to replay this authentication sequence to grant access to the TOE.

7.4 Organisational Security Policies

7.4.1 OSPs drawn from the protection profiles

P.CSP_QCert

Qualified certificate

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. the directive, article 2, clause 9, and Annex I [DIR]) for the SVD generated by the SSCD. The certificates contain at least the name of the signatory and the SVD matching the SCD implemented in the TOE under sole control of the signatory. The CSP ensures that the use of the TOE as SSCD is evident with signatures through the certificate or other publicly available information.

P.QSign

Qualified electronic signatures

The signatory uses a signature creation system to sign data with an advanced electronic signature (cf. the directive, article 1, clause 2 [DIR]), which is a qualified electronic signature if it is based on a valid qualified certificate (according to the directive Annex I [DIR]). The DTBS are presented to the signatory and sent by the SCA as DTBS/R to the SSCD. The SSCD creates the electronic signature created with a SCD implemented in the SSCD that the signatory maintain under their sole control and is linked to the DTBS/R in such a manner that any subsequent change of the data is detectable.

Application Note:

It is a non-qualified advanced electronic signature if it is based on a non-qualified certificate for the SVD.

P.Sigy_SSCD

TOE as secure signature creation device

The TOE meets the requirements for an SSCD laid down in Annex III of the directive [DIR]. This implies the SCD is used for digital signature creation under sole control of the signatory and the SCD can practically occur only once.

P.Sig_Non-Repud

Non-repudiation of signatures

The lifecycle of the SSCD, the SCD and the SVD shall be implemented in a way that the signatory is not able to deny having signed data if the signature is successfully verified with the SVD contained in their unrevoked certificate.

7.5 Assumptions

7.5.1 All SSCD parts

A.CGA

Trustworthy certificate generation application

The CGA protects the authenticity of the signatory's name or pseudonym and the SVD in the (qualified) certificate by an advanced electronic signature of the CSP.

A.SCA

Trustworthy signature creation application

The signatory uses only a trustworthy SCA. The SCA generates and sends the DTBS/R of data the signatory wishes to sign in a form appropriate for signing by the TOE.

7.5.2 Parts 3 and 6 only

A.CSP

Secure SCD/SVD management by CSP

The CSP uses only a trustworthy SCD/SVD generation device and ensures that this device can be used by authorised user only. The CSP ensures that the SCD generated practically occurs only once, that generated SCD and SVD actually correspond to each other and that SCD cannot be derived from the SVD. The CSP ensures the confidentiality of the SCD during generation and export to the TOE, does not use the SCD for creation of any signature and irreversibly deletes the SCD in the operational environment after export to the TOE.

8 Security Objectives

8.1 Security Objectives for the TOE

8.1.1 All SSCD parts

OT.Tamper_Resistance

Tamper resistance

The TOE shall prevent or resist physical tampering with specified system devices and components.

OT.Tamper_ID

Tamper detection

The TOE shall provide system features that detect physical tampering of its components, and uses those features to limit security breaches.

OT.EMSEC_Design

Provide physical emanations security

The TOE shall be designed and built in such a way as to control the production of intelligible emanations within specified limits.

OT.DTBS_Integrity_TOE

DTBS/R integrity inside the TOE

The TOE must not alter the DTBS/R. As by definition of the DTBS/R this may consist of the DTBS themselves, this objective does not conflict with a signature creation process where the TOE hashes the provided DTBS (in part or entirely) for signature creation.

OT.Sigy_SigF

Signature creation function for the legitimate signatory only

The TOE shall provide the digital signature creation function for the legitimate signatory only and protects the SCD against the use of others. The TOE shall resist attacks with high attack potential.

OT.Sig_Secure

Cryptographic security of the electronic signature

The TOE shall create digital signatures that cannot be forged without knowledge of the SCD through robust encryption techniques. The SCD shall not be reconstructable using the digital signatures or any other data exportable from the TOE. The digital signatures shall be resistant against these attacks, even when executed with a high attack potential.

OT.SCD_Secrecy

Secrecy of the signature-creation data

The secrecy of the SCD (used for signature creation) shall be reasonably assured against attacks with a high attack potential.

Application Note:

The TOE shall keep the confidentiality of the SCD at all times, in particular during SCD/SVD generation, signature creation operation, storage and secure destruction.

OT.Lifecycle_Security

Lifecycle security

The TOE shall detect flaws during the initialization, personalization and operational usage. The TOE shall securely destroy the SCD on demand of the signatory.

Application Note:

The TOE may contain more than one set of SCD. There is no need to destroy the SCD in case of repeated SCD generation. The signatory shall be able to destroy the SCD stored in the SSCD e.g. after the (qualified) certificate for the corresponding SVD has been expired.

8.1.2 SSCD parts 2 and additions from 5 only

OT.SCD_SVD_Corresp

Correspondence between SVD and SCD

The TOE shall ensure the correspondence between the SVD and the SCD generated by the TOE. This includes unambiguous reference of a created SVD/SCD pair for export of the SVD and in creating an electronic signature creation with the SCD.

OT.SCD_Unique

Uniqueness of the signature creation data

The TOE shall ensure the cryptographic quality of an SCD/SVD pair it creates as suitable for the advanced or qualified electronic signature. The SCD used for signature creation shall practically occur only once and shall not be reconstructable from the SVD. In that context 'practically occur once' means that the probability of equal SCDs is negligible.

OT.SCD/SVD_Auth_Gen

Authorized SCD/SVD generation

The TOE shall provide security features to ensure that authorised users only may invoke the generation of the SCD and the SVD.

8.1.3 SSCD parts 3 only

OT.SCD_Auth_Imp

Authorized SCD import

The TOE shall provide security features to ensure that authorised users only may invoke the import of the SCD.

8.1.4 Additional Security Objectives for SSCD parts 5 only

OT.TOE_TC_DTBS_Imp

Trusted channel of TOE for DTBS import

The TOE shall provide a trusted channel to the SCA to detect alteration of the DTBS/R received from the SCA. The TOE must not generate electronic signatures with the SCD for altered DTBS.

8.1.5 Additional Security Objectives for the TOE

OT.Authentication_Secure

Secure authentication mechanisms

The TOE provides strong mechanism to authenticate external users/entity and mechanisms to establish a strong trusted channel with an external IT entity. The authentication protocols rely on cryptographic schemes that are based on either symmetric or asymmetric cryptography. The TOE uses freshly generated random number in the authentication mechanism in order to avoid replay attacks. The authentication protocols ensure that the cryptogram cannot be forged without the knowledge of the authentication key, and that they cannot be reconstructed from the authentication cryptograms. The trusted channel ensures integrity, authenticity, and confidentiality of the data using strong encryption techniques. The trusted channel ensures protection against deletion, and modification of commands. Moreover, the TOE ensures the key its uses are genuine by enforcing an access control over the authentication keys update, in order to ensure that only entitled entities can change key values

OT.Lifecycle_Management

Management of the life cycle

The TOE provides a life cycle management enabling to separate its life cycle in two main phases. The first one (phase 6) is the one during the TOE is under the sole control of the Personalization Agent. The following operation may be realized:

- The SCD, SVD and keys may be created, generated, imported or erased
- The RAD (s) may be created and loaded
- SVD and public keys may be exported Once performed, the Personalization Agent switches the TOE in phase 7. This transition is irreversible, leaving the TOE under the sole control of the R.Sigy, R.Admin and the TOE_Administrator according to the security rules set by the Personalization Agent.

OT.TOE_AuthKey_Unique

Uniqueness of the TOE authentication key(s)

The TOE shall ensure the cryptographic quality of the asymmetric authentication key pair used for the TOE authentication. The private key used for TOE authentication can practically occur only once and cannot be reconstructed from the public key. In that context 'practically occur once' means that the probability of equal TOE authentication key is negligible low.

8.2 Security Objectives for the Operational Environment

8.2.1 All SSCD parts

OE.Signatory

Security obligation of the signatory

The signatory shall check that the SCD stored in the SSCD received from SSCD-provisioning service is in non-operational state. The signatory shall keep their VAD confidential.

OE.DTBS_Intend

SCA sends data intended to be signed

The signatory shall use a trustworthy SCA that

- o generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form which is appropriate for signing by the TOE,
- o sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE,
- o attaches the signature produced by the TOE to the data or provides it separately.

Application Note:

The SCA should be able to support advanced electronic signatures. Currently, there exist three formats defined by ETSI recognized as meeting the requirements needed by advanced electronic signatures: CAdES, XAdES and PAdES. These three formats mandate to include the hash of the signer's public key certificate in the data to be signed. In order to support for the mobility of the signer, it is recommended to store the certificate info on the SSCD for use by SCA and identification of the corresponding SCD if more than one SCD is stored on the SSCD.

OE.SVD_Auth

Authenticity of the SVD The operational environment shall ensure the integrity of the SVD sent to the CGA of the CSP. The CGA verifies the correspondence between the SCD in the SSCD of the signatory and the SVD in the qualified certificate.

OE.CGA_QCert

Generation of qualified certificates

The CGA shall generate a qualified certificate that includes (amongst others)

- o the name of the signatory controlling the TOE,
- o the SVD matching the SCD stored in the TOE and being under sole control of the signatory,
- o the advanced signature of the CSP.

The CGA shall confirm with the generated qualified certificate that the SCD corresponding to the SVD is stored in a SSCD.

8.2.2 SSCD parts 2 and 3 only

OE.HID_VAD

Protection of the VAD

If an external device provides the human interface for user authentication, this device will ensure confidentiality and integrity of the VAD as needed by the authentication method employed from import through its human interface until import through the TOE interface.

OE.DTBS_Protect

SCA protects the data intended to be signed

The operational environment ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE.

8.2.3 SSCD part 2, 3 only

OE.SSCD_Prov_Service

Authentic SSCD provided by SSCD Provisioning Service

The SSCD-provisioning service shall initialize and personalize for the signatory an authentic copy of the TOE and deliver this copy as SSCD to the signatory.

8.2.4 SSCD parts 3 only

OE.SCD_SVD_Corresp

Correspondence between SVD and SCD

The CSP shall ensure the correspondence between the SVD and the SCD generated by the CSP. This includes the correspondence between the SVD sent to the CGA and the SCD exported to the TOE of the signatory identified in the SVD certificate.

OE.SCD_Unique

Uniqueness of the signature creation data

The CSP shall ensure the cryptographic quality of the SCD/SVD pair, which is generated in the environment, for the qualified or advanced electronic signature. The SCD used for signature creation shall practically occur only once, i.e. the probability of equal SCDs shall be negligible, and the SCD shall not be reconstructable from the SVD.

OE.SCD_Secrecy

SCD Secrecy

The CSP shall protect the confidentiality of the SCD during generation and export to the TOE. The CSP shall not use the SCD for creation of any signature and shall irreversibly delete the SCD in the operational environment after export to the TOE.

OE.SCD/SVD_Auth_Gen

Authorized SCD/SVD generation

The CSP shall provide security features to ensure that authorised users only may invoke the generation of the SCD and the SVD.

8.2.5 Additions for SSCD parts 5 only

OE.SCA_TC_DTBS_Exp

Trusted channel of SCA for DTBS export

The SCA provides a trusted channel to the TOE for the protection of the integrity of the DTBS to ensure that the DTBS/R cannot be altered undetected in transit between the SCA and the TOE.

Application Note:

This security objective for the TOE is partly covering OE.DTBS_Protect from the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI). While OE.DTBS_Protect in the core PPs (PP Part2 SSCD KG and PP Part3 SSCD KI) requires only the operational environment to protect DTBS, this ST requires the SCA and the TOE to implement a trusted channel for the protection of the DTBS: the SCA exports the DTBS and establishes one end of the trusted channel according to OE.SCA_TC_DTBS_Exp, the TOE imports DTBS at the other end of the trusted channel according to OT.TOE_TC_DTBS_Imp. Therefore this ST re-assigns partly the DTBS protection from the operational environment as described by OE.DTBS_Protect to the TOE as described by OT.TOE_TC_DTBS_Imp and leaves only the necessary functionality by the SCA.

8.3 Security Objectives Rationale

8.3.1 Threats

8.3.1.1 Threats drawn from the protection profiles

T.SCD_Divulg addresses the threat against the legal validity of electronic signature due to storage and copying of SCD outside the TOE, as expressed in the directive [DIR], recital (18). This threat is countered by

- OE.SCD_Secrecy, which assures the secrecy of the SCD in the CSP environment, and
- OT.SCD_Secrecy, which assures the secrecy of the SCD during use by the TOE for signature creation.

Furthermore, generation and/or import of SCD known by an attacker is countered by OE.SCD/SVD_Auth_Gen, which ensures that only authorized SCD generation in the environment is possible, and OT.SCD_Auth_Imp, which ensures that only authorised SCD import is possible.

T.SCD_Derive deals with attacks on the SCD via public known data produced by the TOE, which are the SVD and the signatures created with the SCD. OT.SCD/SVD_Gen counters this threat by implementing cryptographically secure generation of the SCD/SVD pair. OT.Sig_Secure ensures cryptographically secure electronic signatures. OE.SCD_Unique counters this threat by implementing cryptographically secure generation of the SCD/SVD pair.

T.Hack_Phys deals with physical attacks exploiting physical vulnerabilities of the TOE. OT.SCD_Secrecy preserves the secrecy of the SCD. OT.EMSEC_Design counters physical attacks through the TOE interfaces and observation of TOE emanations. OT.Tamper_ID and OT.Tamper_Resistance counter the threat T.Hack_Phys by detecting and by resisting tampering attacks.

T.SVD_Forgery deals with the forgery of the SVD exported by the TOE to the CGA for certificate generation. T.SVD_Forgery is addressed by OT.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD and unambiguous reference of the SVD/SCD pair for the SVD export and signature creation with the SCD, and OE.SVD_Auth that ensures the integrity of the SVD exported by the TOE to the CGA.

OE.SCD_SVD_Corresp, which ensures correspondence between SVD and SCD.

T.SigF_Misuse addresses the threat of misuse of the TOE signature creation function to create SDO by others than the signatory to create an electronic signature on data for which the signatory has not expressed the intent to sign, as required by paragraph 1(c) of Annex III [DIR]. OT.Lifecycle_Security (Lifecycle security) requires the TOE to detect flaws during the initialisation, personalization and operational usage including secure destruction of the SCD, which may be initiated by the signatory. OT.Sigy_SigF (Signature creation function for the legitimate signatory only) ensures that the TOE provides the signature creation function for the legitimate signatory only. OE.DTBS_Intend (Data intended to be signed) ensures that the SCA sends the DTBS/R only for data the signatory intends to sign. OE.DTBS_Protect counters manipulation of the DTBS during transmission over the channel between the SCA and the TOE for SSCD parts 2 and 3 only. For the others SSCD parts, OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. OE.Signatory ensures that the signatory checks that an SCD

stored in the SSCD when received from an SSCD-provisioning service provider is in non-operational state, i.e. the SCD cannot be used before the signatory becomes control over the SSCD. OE.Signatory ensures also that the signatory keeps their VAD confidential.

The combination of OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) and OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS) counters the undetected manipulation of the DTBS during the transmission from the SCA to the TOE.

OT.Lifecycle_Management ensures that when the TOE is under the Personalization Agent control, it can not be misused to sign on behalf of the legitimate Signatory.

T.DTBS_Forgery addresses the threat arising from modifications of the data sent as input to the TOE's signature creation function that does not represent the DTBS as presented to the signatory and for which the signature has expressed its intent to sign. The TOE IT environment addresses T.DTBS_Forgery by the means of OE.DTBS_Intend, which ensures that the trustworthy SCA generates the DTBS/R of the data that has been presented as DTBS and which the signatory intends to sign in a form appropriate for signing by the TOE, and by means of OE.DTBS_Protect, which ensures that the DTBS/R can not be altered in transit between the SCA and the TOE for SSCD parts 2 and 3 only. For the others SSCD parts, the TOE counters this threat by the means of OT.DTBS_Integrity_TOE by ensuring the integrity of the DTBS/R inside the TOE.

The threat T.DTBS_Forgery is addressed by the security objectives OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) and OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS), which ensure that the DTBS/R is sent through a trusted channel and cannot be altered undetected in transit between the SCA and the TOE.

T.Sig_Forgery deals with non-detectable forgery of the electronic signature. OT.Sig_Secure, OT.SCD_Unique and OE.CGA_QCert address this threat in general. OT.Sig_Secure (Cryptographic security of the electronic signature) ensures by means of robust cryptographic techniques that the signed data and the electronic signature are securely linked together. OT.SCD_Unique ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance. OE.CGA_QCert prevents forgery of the certificate for the corresponding SVD, which would result in false verification decision concerning a forged signature.

OE.SCD_Unique ensures that the same SCD cannot be generated more than once and the corresponding SVD cannot be included in another certificate by chance.

T.Authentication_Replay deals with the threats when an attacker retrieves an authentication cryptogram presented to the TOE by an entity and presents it again to the TOE in order to grant some rights and gain access to some data on the TOE. This threat is addressed by OT.Authentication_Secure that ensures the authentication cryptogram can not be replayed as they rely on random data internally generated by the TOE. OT.TOE_AuthKey_Unique ensures the uniqueness of the key.

8.3.2 Organisational Security Policies

8.3.2.1 OSPs drawn from the protection profiles

P.CSP_QCert establishes the CSP generating qualified certificate or non-qualified certificate linking the signatory and the SVD implemented in the SSCD under sole control of this signatory. P.CSP_QCert is addressed by

- OT.Lifecycle_Security, which requires the TOE to detect flaws during the initialisation, personalization and operational usage,

- OT.SCD_SVD_Corresp, which requires to ensure the correspondence between the SVD and the SCD during their generation,
- OE.SCD/SVD_Auth_Gen, which ensures that the SCD/SVD generation can be invoked by authorized users only,
- OT.SCD_Auth_Imp which ensures that authorised users only may invoke the import of the SCD,
- OE.SCD_SVD_Corresp, which requires the CSP to ensure the correspondence between the SVD and the SCD during their generation, and
- OE.CGA_QCert for generation of qualified certificates or non-qualified certificates, which requires the CGA to certify the SVD matching the SCD implemented in the TOE under sole control of the signatory.

P.QSign provides that the TOE and the SCA may be employed to sign data with an advanced electronic signature, which is a qualified electronic signature if based on a valid qualified certificate. OT.Sigy_SigF ensures signatory's sole control of the SCD by requiring the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others. OT.Sig_Secure ensures that the TOE creates electronic signatures, which cannot be forged without knowledge of the SCD through robust encryption techniques. OE.CGA_QCert addresses the requirement of qualified or non-qualified electronic certificates building a base for the electronic signature. OE.DTBS_Intend ensures that the SCA provides only those DTBS to the TOE, which the signatory intends to sign.

P.Sigy_SSCD requires the TOE to meet Annex III [DIR]. This is ensured as follows:

- OE.SCD_Unique meets the paragraph 1(a) of the directive [DIR], Annex III, by the requirements that the SCD used for signature creation can practically occur only once;
- OT.SCD_Unique meets the paragraph 1(a) of Annex III [DIR], by the requirements that the SCD used for signature creation can practically occur only once;
- OT.SCD_Unique, OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(a) of Annex III [DIR] by the requirements to ensure secrecy of the SCD.
- OT.EMSEC_Design and OT.Tamper_Resistance address specific objectives to ensure secrecy of the SCD against specific attacks;
- OT.SCD_Auth_Imp, which limits SCD import to authorized users only;
- OE.SCD_Secrecy, which ensures the confidentiality of the SCD during generation and export to the TOE, and deletes the SCD after export to the TOE. The CSP does not use the SCD for signature creation;
- OT.SCD_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(b) of Annex III [DIR] by the requiements to ensure that the SCD cannot be derived from SVD, the electronic signatures or any other data exported outside the TOE;
- OT.Sigy_SigF meets the requirement in paragraph 1(c) of Annex III [DIR] by the requirements to ensure that the TOE provides the signature creation function for the legitimate signatory only and protects the SCD against the use of others;
- OT.DTBS_Integrity_TOE meets the requirements in paragraph 2 of Annex III [DIR] as the TOE must not alter the DTBS/R.

Paragraph 2 of Annex III [DIR], requires that an SSCD does not prevent the data to be signed from being presented to the signatory prior to the signature process is obviously fulfilled by the method of TOE usage: the SCA will present the DTBS to the signatory and send it to the SSCD for signing.

The usage of SCD under sole control of the signatory is ensured by

- OT.Lifecycle_Security requiring the TOE to detect flaws during the initialisation, personalization and operational usage,
- OE.SCD/SVD_Auth_Gen, which limits invocation of the generation of the SCD and the SVD to authorised users only,
- OT.SCD/SVD_Gen, which limits invocation of the generation of the SCD and the SVD to authorised users only, and
- OT.Sigy_SigF, which requires the TOE to provide the signature creation function for the legitimate signatory only and to protect the SCD against the use of others.

P.Sig_Non-Repud deals with the repudiation of signed data by the signatory, although the electronic signature is successfully verified with the SVD contained in their certificate valid at the time of signature creation. This policy is implemented by the combination of the security objectives for the TOE and its operational environment, which ensures the aspects of signatory's sole control over and responsibility for the electronic signatures created with the TOE.

OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy and OE.SCD_Unique ensure the security of the SCD in the CSP environment. OE.SCD_Secrecy ensures the confidentiality of the SCD during generation, during and after export to the TOE. The CSP does not use the SCD for creation of any signature and deletes the SCD irreversibly after export to the TOE. OE.SCD_Unique provides that the signatory's SCD can practically occur just once. OE.SCD_SVD_Corresp ensures that the SVD in the certificate of the signatory corresponds to the SCD that is implemented in the copy of the TOE of the signatory.

OE.SSCD_Prov_Service ensures that the signatory uses an authentic TOE, initialized and personalized for the signatory for SSCD parts 2,3, 5 only.

OE.CGA_QCert ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory. OE.SVD_Auth and OE.CGA_QCert require the environment to ensure authenticity of the SVD as being exported by the TOE and used under sole control of the signatory. OT.SCD_SVD_Corresp ensures that the SVD exported by the TOE corresponds to the SCD that is implemented in the TOE. OT.SCD_Unique provides that the signatory's SCD can practically occur just once. OE.Signatory ensures that the signatory checks that the SCD, stored in the SSCD received from an SSCD provisioning service is in non-operational state (i.e. the SCD cannot be used before the signatory becomes into sole control over the SSCD). OT.Sigy_SigF provides that only the signatory may use the TOE for signature creation. As prerequisite OE.Signatory ensures that the signatory keeps their VAD confidential. OE.DTBS_Intend and OT.DTBS_Integrity_TOE ensure that the TOE creates electronic signatures only for those DTBS/R, which the signatory has decided to sign as DTBS. The robust cryptographic techniques required by OT.Sig_Secure ensure that only this SCD may create a valid electronic signature that can be successfully verified with the corresponding SVD used for signature verification. The security objective for the TOE OT.Lifecycle_Security (Lifecycle security), OT.SCD_Secrecy (Secrecy of the signature creation data), OT.EMSEC_Design (Provide physical emanations security), OT.Tamper_ID (Tamper detection) and OT.Tamper_Resistance (Tamper resistance) protect the SCD against any compromise.

OE.DTBS_Intend (SCA sends data intended to be signed), OE.DTBS_Protect for SSCD parts 2, 3, 5 only, it ensures that the DTBS/R cannot be altered in transit between the SCA and the TOE, for the others SSCD parts, OT.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE), OE.SCA_TC_DTBS_Exp (Trusted channel of SCA for DTBS) and OT.TOE_TC_DTBS_Imp (Trusted channel of TOE for DTBS) ensure that the TOE generates electronic signatures only for a DTBS/R that the signatory has decided to sign as DTBS.

OT.Lifecycle_Management ensures that when the TOE is under the Personalization Agent control, it cannot be misused to sign on behalf of the legitimate Signatory.

8.3.3 Assumptions

8.3.3.1 All SSCD parts

A.CGA establishes the protection of the authenticity of the signatory's name and the SVD in the qualified certificate by the advanced signature of the CSP by means of the CGA. This is addressed by OE.CGA_QCert (Generation of qualified certificates), which ensures the generation of qualified certificates, and by OE.SVD_Auth (Authenticity of the SVD), which ensures the protection of the integrity of the received SVD and the verification of the correspondence between the SVD and the SCD that is implemented by the SSCD of the signatory.

A.SCA establishes the trustworthiness of the SCA with respect to generation of DTBS/R. This is addressed by OE.DTBS_Intend (Data intended to be signed) which ensures that the SCA generates the DTBS/R of the data that have been presented to the signatory as DTBS and which the signatory intends to sign in a form which is appropriate for being signed by the TOE.

8.3.3.2 Parts 3 only

A.CSP establishes several security aspects concerning handling of SCD and SVD by the CSP. That the SCD/SVD generation device can only be used by authorized users is addressed by OE.SCD/SVD_Auth_Gen (Authorized SCD/SVD Generation), that the generated SCD is unique and cannot be derived by the SVD is addressed by OE.SCD_Unique (Uniqueness of the signature creation data), that SCD and SVD correspond to each other is addressed by OE.SCD_SVD_Corresp (Correspondence between SVD and SCD), and that the SCD are kept confidential, are not used for signature generation in the environment and are deleted in the environment once exported to the TOE is addressed by OE.SCD_Secrecy (SCD Secrecy).

8.3.4 SPD and Security Objectives

Threats	Security Objectives	Rationale
T.SCD_Divulg	OT.SCD_Secrecy, OT.SCD_Auth_Imp, OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy	Section 7.3.1
T.SCD_Derive	OT.SCD/SVD_Gen, OT.Sig_Secure, OE.SCD_Unique	Section 7.3.1
T.Hack_Phys	OT.SCD_Secrecy, OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance	Section 7.3.1
T.SVD_Forgery	OT.SCD_SVD_Corresp, OE.SVD_Auth, OE.SCD_SVD_Corresptok100	Section 7.3.1
T.SigF_Misuse	OT.Lifecycle_Security, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, OE.Signatory, OE.DTBS_Intend OT.TOE_TC_DTBS_Imp, , OE.SCA_TC_DTBS_Exp, OT.Lifecycle_Management, OE.HID_VAD, OE.DTBS_Protect	Section 7.3.1

T.DTBS_Forgery	OT.DTBS_Integrity_TOE, OE.DTBS_Intend, OT.TOE_TC_DTBS_Imp, OE.SCA_TC_DTBS_Exp, OE.DTBS_Protect	Section 7.3.1
T.Sig_Forgery	OT.SCD_Unique, OT.Sig_Secure, OE.CGA_QCert, OE.SCD_Unique	Section 7.3.1
T.Authentication_Replay	OT.Authentication_Secure, OT.TOE_AuthKey_Unique	Section 7.3.1

Table 6 Threats and Security Objectives - Coverage

Security Objectives	Threats	Rationale
OT.Tamper_Resistance	T.Hack_Phys	
OT.Tamper_ID	T.Hack_Phys	
OT.EMSEC_Design	T.Hack_Phys	
OT.DTBS_Integrity_TOE	T.SigF_Misuse, T.DTBS_Forgery	
OT.Sigy_SigF	T.SigF_Misuse	
OT.Sig_Secure	T.SCD_Derive, T.Sig_Forgery	
OT.SCD_Secrecy	T.SCD_Divulg, T.Hack_Phys	
OT.Lifecycle_Security	T.SigF_Misuse	
OT.SCD_SVD_Corresp	T.SVD_Forgery	
OT.SCD_Unique	T.Sig_Forgery	
OT.SCD/SVD_Gen	T.SCD_Derive	
OT.SCD_Auth_Imp	T.SCD_Divulg	
OT.TOE_TC_DTBS_Imp	T.SigF_Misuse, T.DTBS_Forgery	
OT.Authentication_Secure	T.Authentication_Replay	
OT.TOE_AuthKey_Unique	T.Authentication_Replay	
OT.Lifecycle_Management	T.SigF_Misuse	
OE.Signatory	T.SigF_Misuse	
OE.DTBS_Intend	T.SigF_Misuse, T.DTBS_Forgery	
OE.SVD_Auth	T.SVD_Forgery	
OE.CGA_QCert	T.Sig_Forgery	
OE.SCD_SVD_Corresp	T.SVD_Forgery	
OE.SCD_Unique	T.SCD_Derive, T.Sig_Forgery	
OE.SCD_Secrecy	T.SCD_Divulg	
OE.SCD/SVD_Auth_Gen	T.SCD_Divulg	
OE.HID_VAD	T.SigF_Misuse	
OE.SCA_TC_DTBS_Exp	T.SigF_Misuse, T.DTBS_Forgery	

Table 7 Security Objectives and Threats - Coverage

Organisational Security Policies	Security Objectives	Rationale
P.CSP_QCert	OT.Lifecycle_Security, OT.SCD_SVD_Corresp, OE.CGA_QCert, OT.SCD_Auth_Imp, OE.SCD/SVD_Auth_Gen, OE.SCD_SVD_Corresptok99tok135	Section 7.3.2
P.QSign	OT.Sig_Secure, OT.Sigy_SigF, OE.CGA_QCert, OE.DTBS_Intend	Section 7.3.2
P.Sigy_SSCD	OT.Lifecycle_Security, OT.SCD/SVD_Gen, OT.SCD_Unique, OT.SCD_Secrecy, OT.Sig_Secure, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, OT.EMSEC_Design, OT.Tamper_Resistance, OT.SCD_Auth_Imp, OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy, OE.SCD_Unique, tok133 OE.SSCD_Prov_Service	Section 7.3.2
P.Sig_Non-Repud	OT.Lifecycle_Security, OT.SCD_Unique, OT.SCD_SVD_Corresp, OT.SCD_Secrecy, OT.Sig_Secure, OT.Sigy_SigF, OT.DTBS_Integrity_TOE, OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance, OE.CGA_QCert, OE.SVD_Auth, OE.DTBS_Intend, OE.Signatory, OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy, OE.SCD_Unique, OE.SCD_SVD_Corresp, tok133 OT.TOE_TC_DTBS_Imp, OE.SCA_TC_DTBS_Exp, OT.Lifecycle_Management, OE.DTBS_Protect, OE.SSCD_Prov_Service	Section 7.3.2

Table 8 OSPs and Security Objectives - Coverage

Security Objectives	Organisational Security Policies	Rationale
OT.Tamper_Resistance	P.Sigy_SSCD, P.Sig_Non-Repud	
OT.Tamper_ID	P.Sig_Non-Repud	
OT.EMSEC_Design	P.Sigy_SSCD, P.Sig_Non-Repud	
OT.DTBS_Integrity_TOE	P.Sigy_SSCD, P.Sig_Non-Repud	
OT.Sigy_SigF	P.QSign, P.Sigy_SSCD, P.Sig_Non-Repud	
OT.Sig_Secure	P.QSign, P.Sigy_SSCD, P.Sig_Non-Repud	
OT.SCD_Secrecy	P.Sigy_SSCD, P.Sig_Non-Repud	
OT.Lifecycle_Security	P.CSP_QCert, P.Sigy_SSCD, P.Sig_Non-Repud	
OT.SCD_SVD_Corresp	P.CSP_QCert, P.Sig_Non-Repud	
OT.SCD_Unique	P.Sigy_SSCD, P.Sig_Non-Repud	
OT.SCD/SVD_Gen	P.Sigy_SSCD	
OT.SCD_Auth_Imp	P.CSP_QCert, P.Sigy_SSCD	
OT.TOE_TC_DTBS_Imp	P.Sig_Non-Repud	
OT.Authentication_Secure		
OT.Lifecycle_Management	P.Sig_Non-Repud	
OT.TOE_AuthKey_Unique		
OE.Signatory	P.Sig_Non-Repud	
OE.DTBS_Intend	P.QSign, P.Sig_Non-Repud	
OE.SVD_Auth	P.Sig_Non-Repud	
OE.CGA_QCert	P.CSP_QCert, P.QSign, P.Sig_Non-Repud	
OE.SCD_SVD_Corresp	P.CSP_QCert, P.Sig_Non-Repud	
OE.SCD_Unique	P.Sigy_SSCD, P.Sig_Non-Repud	
OE.SCD_Secrecy	P.Sigy_SSCD, P.Sig_Non-Repud	
OE.SCD/SVD_Auth_Gen	P.CSP_QCert, P.Sigy_SSCD, P.Sig_Non-Repud	
OE.SCA_TC_DTBS_Exp	P.Sig_Non-Repud	

Table 9 Security Objectives and OSPs - Coverage

Assumptions	Security Objectives for the Operational Environment	Rationale
A.CGA	OE.CGA_QCert, OE.SVD_Auth	Section 7.3.3
A.SCA	OE.DTBS_Intend	Section 7.3.3
A.CSP	OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy, OE.SCD_Unique, OE.SCD_SVD_Corresp	Section 7.3.3

Table 10 Assumptions and Security Objectives for the Operational Environment - Coverage

Security Objectives for the Operational Environment	Assumptions	Rationale
OE.Signatory		
OE.DTBS_Intend	A.SCA	
OE.SVD_Auth	A.CGA	
OE.CGA_QCert	A.CGA	
OE.SCD_SVD_Corresp	A.CSP	
OE.SCD_Unique	A.CSP	
OE.SCD_Secrecy	A.CSP	
OE.SCD/SVD_Auth_Gen	A.CSP	
OE.SCA_TC_DTBS_Exp		

Table 11 Security Objectives for the Operational Environment and Assumptions - Coverage

9 Extended Requirements

None

10 Security Requirements

10.1 Security Functional Requirements

This section describes the requirements imposed on the TOE in order to achieve the security objectives laid down in the previous chapter.

10.1.1 All SSCD parts

10.1.1.1 Protection of the TSF (FPT)

FPT_EMS.1 TOE Emanation

FPT_EMS.1.1

The TSF shall ensure that the TOE does not emit emissions over its attack surface in such amount that these emissions enable access to TSF data and user data as specified in <table>

ID	Emission	Attack surface	TSF data	User data
1	**Electromagnetic fluctuation**	IC limits	-	o **The session keys, keys** o **SCD** o **PIN/PUK** and o **RAD**.
2	**Power consumptions**	IC limits	-	o **The session keys, keys** o **Keys SCD** o **PIN,PUK** and o **RAD**.

Application Note:

This SFR covers the definition in SSCD PPs and extends them by session keys, keys and PIN/PUK as part of the Mobile protocol aspects. This extension does not conflict with the strict conformance to SSCD PPs.

The TOE shall prevent attacks against the secret data of the TOE where the attack is based on external observable physical phenomena of the TOE. Such attacks may be observable at the interfaces of the TOE or may originate from internal operation of the TOE or may originate from an attacker that varies the physical environment under which the TOE operates. The set of measurable physical phenomena is influenced by the technology employed to implement the TOE. Examples of measurable phenomena are variations in the power consumption, the timing of transitions of internal states, electromagnetic radiation due to internal operation, radio emission. Due to the heterogeneous nature of the technologies that may cause such emanations, evaluation against state-of-the-art attacks applicable to the technologies employed by the TOE is assumed. Examples of such attacks are, but are not limited to,

evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, and so on.

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

- **(1) self-test according to FPT_TST fails**
- **(2) card reset or tearing**
- **(3) Security violation detected by Plateform with FAU_ARP.1,**
- **(4) Failure detected by Plateform with FPT_FLS.1/Base**
- **(5) Integrity error detected on RAD, SCD, and Keys**
- **No other failure**.

FPT_PHP.1 Passive detection of physical attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.3 Resistance to physical attack

FPT_PHP.3.1 The TSF shall resist **physical manipulation and physical probing** to the **TSF** by responding automatically such that the SFRs are always enforced.

FPT_TST.1 TSF testing

FPT_TST.1.1 The TSF shall run a suite of the following self tests **during initial start-up and periodically during normal operation** to demonstrate the correct operation of **the TSF: integrity of TSF, correct OS booting.** .

FPT_TST.1.2 The TSF shall provide authorized users with the capability to verify the integrity of **TSF data**.

FPT_TST.1.3 The TSF shall provide authorized users with the capability to verify the integrity of **TSF**.

10.1.1.2 Security management (FMT)

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- **R.Admin**
- **R.Sigy**

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

FMT_SMF.1 Specification of Management Functions

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

- **Creation and modification of RAD,**
- **Enabling the signature creation function,**
- **Modification of the security attribute SCD/SVD management, SCD operational,**
- **Change the default value of the security attribute SCD Identifier,**
- **Initialization,**
- **Personalization,**
- **Configuration,**
- **Resume and unblock the PIN and PUK (if any)**.

Application Note:

There is no default value for SCD Identifier. This SFR covers the definition in SSCD PPs and extends them by Mobile protocol aspects. This extension does not conflict with the strict conformance to SSCD PPs.

FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to **enable** the functions **signature creation function** to **R.Sigy**.

FMT_MSA.1/Admin Management of security attributes

FMT_MSA.1.1/Admin The TSF shall enforce the **SCD/SVD Generation SFP and SCD Import SFP** to restrict the ability to **modify** the security attributes **SCD/SVD management** to **R.Admin**.

FMT_MSA.1/Signatory Management of security attributes

FMT_MSA.1.1/Signatory The TSF shall enforce the **Signature Creation SFP** to restrict the ability to **modify** the security attributes **SCD operational** to **R.Sigy**.

FMT_MSA.2 Secure security attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for **SCD/SVD Management and SCD operational**.

FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the **SCD/SVD Generation SFP, SVD Transfer SFP, SCD Import SFP and Signature Creation SFP** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **R.Admin** to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.4 Security attribute value inheritance

FMT_MSA.4.1 The TSF shall use the following rules to set the value of security attributes:

- **(1) If S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute "SCD operational of the SCD" shall be set to "no" as a single operation**
- **(2) If S.Sigy successfully generates an SCD/SVD pair the security attribute "SCD operational of the SCD" shall be set to "yes" as a single operation**
- **(3) If S.Admin imports SCD while S.Sigy is not currently authenticated, the security attribute "SCD operational" of the SCD shall be set to "no" after import of the SCD as a single operation.**
- **(4) If S.Admin imports SCD while S.Sigy is currently authenticated, the security attribute "SCD operational" of the SCD shall be set to "yes" after import of the SCD as a single operation**
- **(5) S.Sigy or S.Admin can load or generate an SCD/SVD pair in the limit of 4 key pairs.**
- **(6) S.Admin can load a maximum of 4 PINs and a PUK.**

FMT_MTD.1/Admin Management of TSF data

FMT_MTD.1.1/Admin The TSF shall restrict the ability to **create** the **RAD** to **R.Admin**.

FMT_MTD.1/Signatory Management of TSF data

FMT_MTD.1.1/Signatory The TSF shall restrict the ability to **modify** the **RAD** to **R.Sigy**.

FMT_MTD.1/Unblock Management of TSF data

FMT_MTD.1.1/Unblock The TSF shall restrict the ability to **unblock the RAD to R.Admin.**

Application note: This SFR apply to any RAD (belonging to R.Sigy or R.Admin).

10.1.1.3 Identification and authentication (FIA)

FIA_UID.1 Timing of identification

FIA_UID.1.1 The TSF shall allow

- **Self-test according to FPT_TST.1,**
- **Establishing a trusted channel between a trusted IT product generating the SCD/SVD pair for import of the SCD as described by FDP_UCT.1/SCD and FDP_ITC.1/SCD and the TOE by means of TSF required by FTP_ITC.1/SCD (not applicable for SSCD KG).**
- **Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS to send the DTBS ([PP-SSCD5])**

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

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

FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **an administrator configurable positive integer within [1 and 15]** unsuccessful authentication attempts occur related to **consecutive failed authentication attempts**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been **met**, the TSF shall

- **Block RAD**.

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow

- **Self-test according to FPT_TST.1,**
- **Identification of the user by means of TSF required by FIA_UID.1**
- **Establishing a trusted channel between a trusted IT product generating the SCD/SVD pair for import the SCD as described by FDP_UCT.1/SCD and FDP_ITC.1/SCD and the TOE by means of TSF required by FTP_ITC.1/SCD (not applicable for SSCD KG).**
- **Establishing a trusted channel between the SCA and the TOE by means of TSF required by FTP_ITC.1/DTBS to send the DTBS ([PP-SSCD5])**

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

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

10.1.1.4 User data protection (FDP)

The security attributes and related status for the subjects and objects are:

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
S.User	Role	R.Admin, R.Sigy
S.User	SCD/SVD Management	authorised, not authorised
SCD	SCD Operational	no, yes
SCD	SCD identifier	arbitrary value

FDP_SDI.2/DTBS Stored data integrity monitoring and action

FDP_SDI.2.1/DTBS The TSF shall monitor user data stored in containers controlled by the TSF for **integrity error** on all objects, based on the following attributes: **integrity checked stored DTBS**.

FDP_SDI.2.2/DTBS Upon detection of a data integrity error, the TSF shall

- **prohibit the use of the altered data**
- **inform the S.Sigy about integrity error**.

FDP_SDI.2/Persistent Stored data integrity monitoring and action

FDP_SDI.2.1/Persistent The TSF shall monitor user data stored in containers controlled by the TSF for **integrity error** on all objects, based on the following attributes: **integrity checked stored data**.

FDP_SDI.2.2/Persistent Upon detection of a data integrity error, the TSF shall

- **prohibit the use of the altered data**
- **inform the S.Sigy about integrity error**.

FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the **deallocation of the resource from** the following objects:

o Session keys (immediately after closing related communication session),

o SCD key

The following data persistently stored by the TOE shall have the user data attribute "integrity checked persistent stored data":

1. SCD
2. SVD (if persistently stored by the TOE).

The DTBS/R temporarily stored by the TOE has the user data attribute "integrity checked stored data".

FDP_ACC.1/Signature_Creation Subset access control

FDP_ACC.1.1/Signature_Creation The TSF shall enforce the **Signature Creation SFP** on **Sending of DTBS/R by SCA and Signing of DTBS/R by Signatory:**

- **subjects: S.User,**
- **objects: DTBS/R, SCD,**
- **operations: signature creation**.

FDP_ACF.1/Signature_Creation Security attribute based access control

FDP_ACF.1.1/Signature_Creation The TSF shall enforce the **Signature Creation SFP** to objects based on the following:

- **the user S.User is associated with the security attribute "Role" and**
- **the SCD with the security attribute "SCD Operational"**.

FDP_ACF.1.2/Signature_Creation The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **R.Sigy is allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "yes"**.

FDP_ACF.1.3/Signature_Creation The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/Signature_Creation The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **S.User is not allowed to create electronic signatures for DTBS/R with SCD which security attribute "SCD operational" is set to "no"**.

10.1.1.5 Cryptographic support (FCS)

FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[Cryptographic Operation]** in accordance with a specified cryptographic algorithm **[Cryptographic Algorithm]** and cryptographic key sizes **[Cryptographic Key Sizes]** that meet the following: **[Standards]**

Cryptographic Operation	Cryptographic Algorithms	Cryptographic Key Sizes	Standards
Digital signature creation	ECDSA with ECC 256 and SHA2-256, SHA2-384, SHA2-512	ECC keys of 256 bits	ANSI_X9.62-2005
GP Secure messaging - Encryption/decryption	AES in CBC mode	AES:128, 192, 256 bits	[GP], SCP80 [TS_102225], SCP03 [GP].
Secure messaging - CMAC generation and verification	CMAC (AES)	AES: 128, 192, 256 bits	[GP] AES: NIST SP 800-38B ISO/IEC 9797-1 Method 2 padding SCP80 [TS_102225], SCP03 [GP].
Authentication	ECDSA	256 bits	[SEC1] and ANSI_X9.62-2005
Hashing	SHA-1, SHA2-256, SHA2-384, SHA2-512	none	Secure Hash Standard, FIPS PUB 180-3

Application Note:

The applet mobileID uses these cryptographic operations but they are all implemented by the OS.

FCS_CKM.6 Cryptographic key destruction

FCS_CKM.6.1 The TSF shall destroy **keys build with FCS_CKM.1** when **new key is needed**.

FCS_CKM.6.2 The TSF shall destroy cryptographic keys and keying material specified by FCS_CKM.6.1 in accordance with a specified cryptographic key destruction method**:**

overwriting the keys by a new value of a key that meets the following: **new generation of key with FCS_CKM.1 overwrites old key**.

10.1.2 SSCD parts 2, 3 and some extension from 5 only

10.1.2.1 Cryptographic support (FCS)

FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[Cryptographic Key Generation Algorithm]** and specified cryptographic key sizes **[Cryptographic Key Sizes]** that meet the following: **[Standards]**

Cryptographic Key Generation Algorithm	Cryptographic Key Sizes	Standards
ECC key pair generation	256 bits	IEEE Std 1363a-2004

Application Note:

The applet mobileID uses this cryptographic key generation algorithm but it is implemented by the OS.

10.1.2.2 User data protection (FDP)

The security attributes and related status for the subjects and objects are:

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
S.User	Role	R.Admin, R.Sigy
S.User	SCD/SVD Management	authorised, not authorised
SCD	SCD Operational	no, yes
SCD	SCD identifier	arbitrary value

FDP_ACC.1/SVD_Transfer Subset access control

FDP_ACC.1.1/SVD_Transfer The TSF shall enforce the **SVD Transfer SFP** on

- **subjects: S.User,**
- **objects: SVD,**
- **operations: export**.

FDP_ACF.1/SVD_Transfer Security attribute based access control

FDP_ACF.1.1/SVD_Transfer The TSF shall enforce the **SVD Transfer SFP** to objects based on the following:

- **the S.User is associated with the security attribute Role,**
- **the SVD**.

FDP_ACF.1.2/SVD_Transfer The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **R.Admin and R.Sigy is allowed to export SVD**.

FDP_ACF.1.3/SVD_Transfer The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/SVD_Transfer The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **none**.

FDP_ACC.1/SCD/SVD_Generation Subset access control

FDP_ACC.1.1/SCD/SVD_Generation The TSF shall enforce the **SCD/SVD Generation SFP** on

- **subjects: S.User,**
- **objects: SCD, SVD,**
- **operations: generation of SCD/SVD pair**.

FDP_ACF.1/SCD/SVD_Generation Security attribute based access control

FDP_ACF.1.1/SCD/SVD_Generation The TSF shall enforce the **SCD/SVD Generation SFP** to objects based on the following: **the user S.User is associated with the security attribute "SCD/SVD Management"**.

FDP_ACF.1.2/SCD/SVD_Generation The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **S.User with the security attribute "SCD/SVD Management" set to "authorised" is allowed to generate SCD/SVD pair**.

FDP_ACF.1.3/SCD/SVD_Generation The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/SCD/SVD_Generation The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **S.User with the security attribute**

"SCD/SVD management" set to "not authorised" is not allowed to generate SCD/SVD pair.

10.1.3 SSCD parts 3 only

10.1.3.1 Trusted path/channels (FTP)

FTP_ITC.1/SCD Inter-TSF trusted channel

FTP_ITC.1.1/SCD 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/SCD The TSF shall permit **another trusted IT product** to initiate communication via the trusted channel.

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

- **Data exchange integrity according to FDP_UCT.1/SCD**.
- **none**

10.1.3.2 User data protection (FDP)

The security attributes and related status for the subjects and objects are:

Subject or object the security attribute is associated with	Security attribute type	Value of the security attribute
S.User	Role	R.Admin, R.Sigy
S.User	SCD/SVD Management	authorised, not authorised
SCD	SCD Operational	no, yes
SCD	SCD identifier	arbitrary value

FDP_UCT.1/SCD Basic data exchange confidentiality

FDP_UCT.1.1/SCD [Editorially Refined] The TSF shall enforce the **SCD Import SFP** to **receive SCD** in a manner protected from unauthorised disclosure.

FDP_ITC.1/SCD Import of user data without security attributes

FDP_ITC.1.1/SCD The TSF shall enforce the **SCD Import SFP** when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2/SCD [Editorially Refined] The TSF shall ignore any security attributes associated with the **SCD** when imported from outside the TOE.

FDP_ITC.1.3/SCD The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: **The SCD shall be sent by an authorized trusted IT environment**.

FDP_ACC.1/SCD_Import Subset access control

FDP_ACC.1.1/SCD_Import The TSF shall enforce the **SCD Import SFP** on

- **subjects: S.User,**
- **objects: SCD,**
- **operations: import of SCD**.

FDP_ACF.1/SCD_Import Security attribute based access control

FDP_ACF.1.1/SCD_Import The TSF shall enforce the **SCD Import SFP** to objects based on the following: **the user S.User is associated with the security attribute "SCD/SVD Management"**.

FDP_ACF.1.2/SCD_Import The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **S.User with the security attribute "SCD/SVD Management" set to "authorised" is allowed to import SCD**.

FDP_ACF.1.3/SCD_Import The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**.

FDP_ACF.1.4/SCD_Import The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **S.User with the security attribute "SCD/SVD management" set to "not authorised" is not allowed to import SCD**.

10.1.4 Added parts from SSCD 5 only

10.1.4.1 User data protection (FDP)

FDP_UIT.1/DTBS Data exchange integrity

FDP_UIT.1.1/DTBS The TSF shall enforce the **Signature Creation SFP** to **receive** user data in a manner protected from **modification and insertion** errors.

FDP_UIT.1.2/DTBS The TSF shall be able to determine on receipt of user data, whether **modification and insertion** has occurred.

10.1.4.2 Trusted path/channels (FTP)

FTP_ITC.1/DTBS Inter-TSF trusted channel

FTP_ITC.1.1/DTBS [Editorially Refined] The TSF shall provide a communication channel between itself and another trusted IT product **SCA** 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/DTBS [Editorially Refined] The TSF shall permit **the SCA** to initiate communication via the trusted channel.

FTP_ITC.1.3/DTBS [Editorially Refined] The TSF **or the SCA** shall initiate communication via the trusted channel for **signature creation**.

10.1.5 Additional SFRs

FCS_RNG.1 Random number generation

FCS_RNG.1.1 The TSF shall provide a deterministic random number generator that implements **DRG.3 as defined in [AIS]:**

(DRG.3.1) If initialized with a random seed **using a PTRNG as random source** the internal state of the RNG shall **have at least 256 bits of entropy.**

(DRG.3.2) The RNG provides forward secrecy.

(DRG.3.3) The RNG provides backward secrecy even if the current internal state is known.

FCS_RNG.1.2 The TSF shall provide **numbers format 128-bit blocks** that meet:

(DRG.3.4) The RNG, initialized with a random seed **using a PTRNG** generates output for which in 2^35 strings of bit length 128 are mutually different with probability 1-2(-19).

(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.

Application Note:

The applet mobileID uses these random number operations but they are implemented by the OS.

FMT_MTD.1/TOE_State Management of TSF data

FMT_MTD.1.1/TOE state The TSF shall restrict the ability to **switch** the **TOE from phase 6 to phase 7** to **Personalisation_Agent.**

10.2 Security Assurance Requirements

The Evaluation Assurance Level is EAL4 augmented with AVA_VAN.5, ALC_DVS.2 and ALC_FLR.3: see definitions in CC:2022.

10.3 Security Requirements Rationale

10.3.1 Objectives

10.3.1.1 Security Objectives for the TOE

All SSCD parts

OT.Tamper_Resistance is provided by FPT_PHP.3 to resist physical attacks.

OT.Tamper_ID is provided by FPT_PHP.1 by the means of passive detection of physical attacks.

OT.EMSEC_Design covers that no intelligible information is emanated. This is provided by FPT_EMS.1.1.

OT.DTBS_Integrity_TOE ensures that the DTBS/R is not altered by the TOE. The integrity functions specified by FDP_SDI.2/DTBS require that the DTBS/R has not been altered by the TOE.

OT.Sigy_SigF is provided by an SFR for identification authentication and access control.

FIA_UAU.1 and FIA_UID.1 ensure that no signature creation function can be invoked before the signatory is identified and authenticated. The security functions specified by FMT_MTD.1/Admin and FMT_MTD.1/Signatory manage the authentication function. SFR FIA_AFL.1 provides protection against a number of attacks, such as cryptographic extraction of residual information, or brute force attacks against authentication. The security function specified by FDP_SDI.2/DTBS ensures the integrity of stored DTBS and FDP_RIP.1 prevents misuse of any resources containing the SCD after de-allocation (e.g. after the signature creation process).

The security functions specified by FDP_ACC.1/Signature_Creation and FDP_ACF.1/Signature_Creation provide access control based on the security attributes managed according to the SFR FMT_MTD.1/Signatory, FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4. The SFR FMT_SMF.1 and FMT_SMR.1 list these management functions and the roles. These ensure that the signature process is restricted to the signatory. FMT_MOF.1 restricts the ability to enable the signature creation function to the signatory. FMT_MSA.1/Signatory restricts the ability to modify the security attributes SCD operational to the signatory and

FMT_MTD.1/Unblock ensures the unblocking of the RAD is made under the sole control of the administrator. In phase 6, the RAD may be loaded on the TOE by the Personalization Agent as defined in FMT_SMF.1. The Personalization Agent is authenticated with a mutual authentication performed with FCS_RNG.1 and FCS_COP.1, and is authenticated with FMT_SMR.1. During the mutual authentication, a session encryption key is agreed between the TOE and the Personalization Agent and used by the TOE to decrypt the RAD using FCS_COP.1, ensuring the confidentiality of the RAD during its transfer in phase 6. In phase 6, FMT_MSA.1/Signatory guarantees that the Personalization Agent cannot sign on behalf of the signatory, ensuring the signature creation features remains under the sole control of the signatory.

OT.Sig_Secure is provided by the cryptographic algorithms specified by FCS_COP.1, which ensures the cryptographic robustness of the signature algorithms. FDP_SDI.2/Persistent

corresponds to the integrity of the SCD implemented by the TOE and FPT_TST.1 ensures self-tests ensuring correct signature creation.

OT.SCD_Secrecy is provided by the security functions specified by the following SFR. FCS_CKM.1 ensures the use of secure cryptographic algorithms for SCD/SVD generation. Cryptographic quality of SCD/SVD pair shall prevent disclosure of SCD by cryptographic attacks using the publicly known SVD. The security functions specified by FDP_RIP.1 and FCS_CKM.6 ensure that residual information on SCD is destroyed after the SCD has been use for signature creation and that destruction of SCD leaves no residual information.

The security functions specified by FDP_SDI.2/Persistent ensure that no critical data is modified which could alter the efficiency of the security functions or leak information of the SCD. FPT_TST.1 tests the working conditions of the TOE and FPT_FLS.1 guarantees a secure state when integrity is violated and thus assures that the specified security functions are operational. An example where compromising error conditions are countered by FPT_FLS.1 is fault injection for differential fault analysis (DFA). FDP_UCT.1/SCD and FTP_ITC.1/SCD ensures the confidentiality for SCD import.SFR FPT_EMS.1 and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD.

OT.Lifecycle_Security is provided by the SFR for SCD/SVD generation FCS_CKM.1, SCD usage FCS_COP.1 and SCD destruction FCS_CKM.6 which ensure cryptographically secure lifecycle of the SCD. The SCD/SVD generation is controlled by TSF according to FDP_ACC.1/SCD/SVD_Generation and FDP_ACF.1/SCD/SVD_Generation. The SVD transfer for certificate generation is controlled by TSF according to FDP_ACC.1/SVD_Transfer and FDP_ACF.1/SVD_Transfer. The SCD usage is ensured by access control FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation which is based on the security attribute secure TSF management according to FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory, FMT_MTD.1/Unblock, FMT_SMF.1 and FMT_SMR.1. The test functions FPT_TST.1 provides failure detection throughout the lifecycle. The SCD import is controlled by TSF according to FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import and FDP_ITC.1/SCD. The confidentiality of the SCD is protected during import according to FDP_UCT.1/SCD in the trusted channel FTP_ITC.1/SCD.

SSCD parts 2, 3 and additions from part 5 only

OT.SCD_SVD_Corresp addresses that the SVD corresponds to the SCD implemented by the TOE. This is provided by the algorithms specified by FCS_CKM.1 to generate corresponding SVD/SCD pairs. The security functions specified by FDP_SDI.2/Persistent ensure that the keys are not modified, so to retain the correspondence. Moreover, the SCD Identifier allows the environment to identify the SCD and to link it with the appropriate SVD. The management functions identified by FMT_SMF.1 and by FMT_MSA.4 allow R.Admin to modify the default value of the security attribute SCD Identifier.

OT.SCD_Unique implements the requirement of practically unique SCD as laid down in Annex III [DIR], paragraph 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1.

OT.SCD/SVD_Gen addresses that generation of a SCD/SVD pair requires proper user authentication. The TSF specified by FIA_UID.1 and FIA_UAU.1 provide user identification and user authentication prior to enabling access to authorised functions. The SFR FDP_ACC.1/SCD/SVD_Generation and FDP_ACF.1/SCD/SVD_Generation provide access control for the SCD/SVD generation. The security attributes of the authenticated user are

provided by FMT_MSA.1/Admin, FMT_MSA.2, and FMT_MSA.3 for static attribute initialisation. The SFR FMT_MSA.4 defines rules for inheritance of the security attribute 'SCD operational' of the SCD.

SSCD parts 3 only

OT.SCD_Auth_Imp is provided by the security functions specified by the following SFR. FIA_UID.1 and FIA_UAU.1 ensure that the user is identified and authenticated before SCD can be imported. FDP_ACC.1/SCD_Import and FDP_ACF.1/SCD_Import ensure that only authorised users can import SCD.

SSCD additions from part 5 only

OT.TOE_TC_DTBS_Imp is provided by FTP_ITC.1/DTBS to provide a trusted channel to protect the DTBS provided by the SCA to the TOE and by FDP_UIT.1/DTBS, which requires the TSF to verify the integrity of the received DTBS.

Additional Security Objectives for the TOE

OT.Authentication_Secure is provided by the cryptographic algorithms specified by FCS_COP.1 and FCS_RNG.1 for (1) the mutual authentication based on an asymmetric scheme (Device Authentication), (2) the mutual authentication based on symmetric scheme, (3) the authentication of the personalization agent and of the "TOE_Administrator", (4) the authentication of an entity based on a symmetric scheme, (5) the authentication of an entity based on an asymmetric scheme. All these requirements ensure the cryptographic robustness of the authentication mechanisms. The use of a challenge freshly generated by the TOE with FCS_RNG.1 in theses authentication protocols ensures a protection against replay attacks when authenticating external entities. The security function specified by FPT_TST.1 ensures that the security functions are performed correctly and FDP_SDI.2/Persistent guarantees the integrity of the authentication key(s) used by the TOE. FMT_SMR.1 and FMT_SMF.1 ensure the TOE can distinguish between external entities successfully authenticated (R.Admin) and can grant them dedicated rights. FDP_RIP.1 ensures that the key value is not kept by the TOE after usage and then can not be reused for a replay attack.This objective ensures as well the establishment of a trusted channel following a successful mutual authentication ((1) and (2)). This trusted channel ensures authenticity, integrity and confidentiality of communication. FCS_CKM.1 and FCS_COP.1 generate session keys for the secure communication from a common secret agreed between the TOE and the external entity during the mutual authentication procedure. Any incoming command shall contain a MAC computed by the issuer with the session key agreed during the mutual authentication, so that any unauthenticated or non integer command is detected by the MAC verification performed by the TOE using FCS_COP.1. The data exchanged through this trusted channel are also protected in confidentiality thanks to FCS_COP.1, ensuring they can only be disclosed to the parties authenticated during the mutual authentication step. The encryption key is ephemeral as it is generated during the mutual authentication using a challenge freshly generated by the TOE using FCS_RNG.1, which ensures that dictionary attacks cannot be performed on encrypted data. When an integrity error is detected, or if the MAC is wrong (wrong authentication of the command issuer), the session keys (for integrity and confidentiality) are erased thanks to FCS_CKM.6 so that they cannot be reused anymore, causing the trusted channel to be irreversibly lost. In particular, it ensures that encrypted data that may be caught by an attacker cannot be reused anymore to masquerade the TOE. The type of authentication scheme used by the TOE to authenticate the administrator or perform a mutual authentication may be controlled by the "TOE_Administrator". It may enforce the TOE to allow the use of symmetric scheme ((2)

and (4)) and/or asymmetric ((1) and (5)) schemes. The TSF specified by FIA_UID.1 and FIA_UAU.1 provide "TOE_Administrator" identification and authentication prior to enabling access to authorised functions. The attributes of the authenticated "TOE_Administrator" are provided by FMT_MSA.2, FMT_MSA.3 and FMT_MSA.4 for static attribute initialisation. Access control is provided by FMT_SMR.1 and FMT_SMF.1. Effort to bypass the access control by a frontal exhaustive attack is blocked by FIA_AFL.1.

OT.Lifecycle_Management ensures a correct separation of the TOE life cycle between phase 6 and 7. In phase 6, FMT_MTD.1/TOE_State ensures the TOE irreversibly switches from phase 6 to phase 7 under the sole control of the Personalization Agent. The Personalization Agent is authenticated with a mutual authentication performed with FCS_RNG.1 and FCS_COP.1 and is authenticated with FMT_SMR.1. Effort to bypass the access control by a frontal exhaustive attack is blocked by FIA_AFL.1. In phase 7, FDP_ACC.1/Signature_Creation, FDP_ACC.1/SVD_Transfer, FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/SCD_Import, FDP_ACF.1/Signature_Creation, FDP_ACF.1/SVD_Transfer, FDP_ACF.1/SCD/SVD_Generation, FDP_ACF.1/SCD_Import, FMT_MTD.1/Unblock, FMT_MOF.1, FMT_MTD.1/Admin, FMT_MTD.1/Signatory ensures the Personalization Agent does not control the TOE anymore. In phase 6, the Personalization Agent has complete control over the administrative functions of the TOE. It may import, erase, generate SCD/SVD, export SVD, manage Keys, create RAD and manage the configuration of the TOE as mandated in FMT_SMF.1, according to the security policies defined in FDP_ACC.1/SVD_Transfer, FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/SCD_Import, FDP_ACF.1/ SVD_Transfer, FDP_ACF.1/SCD/SVD_Generation, FDP_ACF.1/SCD_Import. It may as well change TOE State (FMT_MTD.1/TOE_State). These functions are protected by the Personalization Agent authentication that cannot be bypassed to access these functions with the TSF specified by FIA_UID.1 and FIA_UAU.1. FMT_MSA.1/Admin, FMT_MSA.2, FMT_MSA.3 ensure that the sole Personalization Agent can realize these functions. Effort to bypass the access control by a frontal exhaustive attack is blocked by FIA_AFL.1.

OT.TOE_AuthKey_Unique is provided by the cryptographic mechanisms specified by FCS_COP.1 for the C/S Authentication. These requirements ensure the cryptographic robustness of these eServices. The eServices keys may be loaded, generated, and the matching public key may be exported as required by FMT_SMF.1. The Agent(s) entitled to perform such operations shall be authenticated with FMT_SMR.1 using cryptographic protocols specified by FCS_COP.1 and FCS_RNG.1 for (1) the mutual authentication based on an asymmetric scheme (Device Authentication), (2) the mutual authentication based on symmetric scheme, (3) the authentication of an entity based on a symmetric scheme, (4) the authentication of an entity based on an asymmetric scheme. These functions are protected by the proper Agent(s) authentication that cannot be bypassed to access these functions with the TSF specified by FIA_UID.1 and FIA_UAU.1.

10.3.2 Rationale tables of Security Objectives and SFRs

Security Objectives	Security Functional Requirements	Rationale
OT.Tamper_Resistance	FPT_PHP.3	Section 9.3.1
OT.Tamper_ID	FPT_PHP.1	Section 9.3.1
OT.EMSEC_Design	FPT_EMS.1	Section 9.3.1
OT.DTBS_Integrity_TOE	FDP_SDI.2/DTBS	Section 9.3.1

OT.Sigy_SigF	FDP_ACF.1/Signature_Creation, FDP_ACC.1/Signature_Creation, FDP_RIP.1, FDP_SDI.2/DTBS, FIA_AFL.1, FIA_UAU.1, FIA_UID.1, FMT_MOF.1, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory, FMT_SMR.1, FMT_SMF.1, FMT_MTD.1/Unblock, FCS_COP.1, tok293 FCS_RNG.1	Section 9.3.1
OT.Sig_Secure	FDP_SDI.2/Persistent, FPT_TST.1, FCS_COP.1	Section 9.3.1
OT.SCD_Secrecy	FCS_CKM.1, FCS_CKM.6, FDP_RIP.1, FDP_SDI.2/Persistent, FPT_FLS.1, FPT_PHP.3, FPT_TST.1, FPT_EMS.1, FDP_UCT.1/SCD, FTP_ITC.1/SCD	Section 9.3.1
OT.Lifecycle_Security	FCS_CKM.1, FCS_CKM.6, FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FDP_ACC.1/SVD_Transfer, FDP_ACF.1/Signature_Creation, FDP_ACC.1/Signature_Creation, FDP_ACF.1/SVD_Transfer, FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory, FMT_SMR.1, FMT_SMF.1, FPT_TST.1, FCS_COP.1, FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import, FDP_ITC.1/SCD, FDP_UCT.1/SCD, FTP_ITC.1/SCD, FMT_MTD.1/Unblock	Section 9.3.1
OT.SCD_SVD_Corresp	FCS_CKM.1, FDP_SDI.2/Persistent, FMT_MSA.4, FMT_SMF.1	Section 9.3.1
OT.SCD_Unique	FCS_CKM.1	Section 9.3.1
OT.SCD/SVD_Gen	FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FIA_UAU.1, FIA_UID.1, FMT_MSA.1/Admin, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4	Section 9.3.1
OT.SCD_Auth_Imp	FIA_UID.1, FIA_UAU.1, FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import	Section 9.3.1
OT.TOE_TC_DTBS_Imp	FDP_UIT.1/DTBS, FTP_ITC.1/DTBS	Section 9.3.1
OT.Authentication_Secure	FPT_TST.1, FMT_SMR.1, FMT_SMF.1, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FIA_UID.1, FIA_AFL.1, FIA_UAU.1, FDP_SDI.2/Persistent, FDP_RIP.1, FCS_COP.1, FCS_CKM.6, FCS_CKM.1, FCS_RNG.1	Section 9.3.1
OT.Lifecycle_Management	FMT_SMR.1, FMT_SMF.1, FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.2, FMT_MSA.3, FMT_MTD.1/Admin, FMT_MTD.1/Signatory, FIA_UID.1, FIA_AFL.1, FIA_UAU.1, FCS_COP.1,	Section 9.3.1

	FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FMT_MTD.1/TOE_State , FCS_RNG.1, FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import, FMT_MTD.1/Unblock, FDP_ACC.1/SVD_Transfer, FDP_ACF.1/Signature_Creation, FDP_ACC.1/Signature_Creation	
OT.TOE_AuthKey_Unique	FMT_SMR.1, FMT_SMF.1, FIA_UID.1, FIA_UAU.1, FCS_COP.1, FCS_RNG.1	Section 9.3.1

Table 12 Security Objectives and SFRs - Coverage

Security Functional Requirements	Security Objectives	Rationale
FPT_EMS.1	OT.EMSEC_Design, OT.SCD_Secrecy,	
FPT_FLS.1	OT.SCD_Secrecy	
FPT_PHP.1	OT.Tamper_ID	
FPT_PHP.3	OT.Tamper_Resistance, OT.SCD_Secrecy	
FPT_TST.1	OT.Sig_Secure, OT.SCD_Secrecy, OT.Lifecycle_Security, OT.Authentication_Secure	
FMT_SMR.1	OT.Sigy_SigF, OT.Lifecycle_Security, OT.Authentication_Secure, OT.Lifecycle_Management, OT.TOE_AuthKey_Unique	
FMT_SMF.1	OT.Sigy_SigF, OT.Lifecycle_Security, OT.SCD_SVD_Corresp, OT.Authentication_Secure, OT.Lifecycle_Management, OT.TOE_AuthKey_Unique	
FMT_MOF.1	OT.Sigy_SigF, OT.Lifecycle_Security, OT.Lifecycle_Management	
FMT_MSA.1/Admin	OT.Lifecycle_Security, OT.SCD/SVD_Gen, OT.Lifecycle_Management	
FMT_MSA.1/Signatory	OT.Sigy_SigF, OT.Lifecycle_Security	
FMT_MSA.2	OT.Sigy_SigF, OT.Lifecycle_Security, OT.SCD/SVD_Gen, OT.Authentication_Secure, OT.Lifecycle_Management	
FMT_MSA.3	OT.Sigy_SigF, OT.Lifecycle_Security, OT.SCD/SVD_Gen, OT.Authentication_Secure, OT.Lifecycle_Management	
FMT_MSA.4	OT.Sigy_SigF, OT.Lifecycle_Security, OT.SCD_SVD_Corresp,	

	OT.SCD/SVD_Gen, OT.Authentication_Secure	
FMT_MTD.1/Admin	OT.Sigy_SigF, OT.Lifecycle_Security, OT.Lifecycle_Management	
FMT_MTD.1/Signatory	OT.Sigy_SigF, OT.Lifecycle_Security, OT.Lifecycle_Management	
FIA_UID.1	OT.Sigy_SigF, OT.SCD/SVD_Gen, OT.SCD_Auth_Imp, OT.Authentication_Secure, OT.Lifecycle_Management, OT.TOE_AuthKey_Unique	
FIA_AFL.1	OT.Sigy_SigF, OT.Authentication_Secure, OT.Lifecycle_Management	
FIA_UAU.1	OT.Sigy_SigF, OT.SCD/SVD_Gen, OT.SCD_Auth_Imp, OT.Authentication_Secure, OT.Lifecycle_Management, OT.TOE_AuthKey_Unique	
FDP_SDI.2/DTBS	OT.DTBS_Integrity_TOE, OT.Sigy_SigF	
FDP_SDI.2/Persistent	OT.Sig_Secure, OT.SCD_Secrecy, OT.SCD_SVD_Corresp, OT.Authentication_Secure	
FDP_RIP.1	OT.Sigy_SigF, OT.SCD_Secrecy, OT.Authentication_Secure	
FDP_ACC.1/Signature_Creation	OT.Sigy_SigF, OT.Lifecycle_Security	
FDP_ACF.1/Signature_Creation	OT.Sigy_SigF, OT.Lifecycle_Security	
FCS_COP.1	OT.Sigy_SigF, OT.Sig_Secure, OT.Lifecycle_Security, OT.Authentication_Secure, OT.Lifecycle_Management, OT.TOE_AuthKey_Unique	
FCS_CKM.6	OT.SCD_Secrecy, OT.Lifecycle_Security, OT.Authentication_Secure	
FCS_CKM.1	OT.SCD_Secrecy, OT.Lifecycle_Security, OT.SCD_SVD_Corresp, OT.SCD_Unique, OT.Authentication_Secure	
FDP_ACC.1/SVD_Transfer	OT.Lifecycle_Securitytok100	
FDP_ACF.1/SVD_Transfer	OT.Lifecycle_Security	
FDP_ACC.1/SCD/SVD_Generation	OT.Lifecycle_Security, OT.SCD/SVD_Gen, OT.Lifecycle_Management	
FDP_ACF.1/SCD/SVD_Generation	OT.Lifecycle_Security, OT.SCD/SVD_Gen, OT.Lifecycle_Management	

FTP_ITC.1/SCD	OT.SCD_Secrecy, OT.Lifecycle_Security	
FDP_UCT.1/SCD	OT.SCD_Secrecy, OT.Lifecycle_Security	
FDP_ITC.1/SCD	OT.Lifecycle_Security	
FDP_ACC.1/SCD_Import	OT.Lifecycle_Security, OT.SCD_Auth_Imp	
FDP_ACF.1/SCD_Import	OT.Lifecycle_Security, OT.SCD_Auth_Imp	
FDP_UIT.1/DTBS	OT.TOE_TC_DTBS_Imp	
FTP_ITC.1/DTBS	OT.TOE_TC_DTBS_Imp	
FCS_RNG.1	OT.Sigy_SigF, OT.Authentication_Secure, OT.Lifecycle_Management, OT.TOE_AuthKey_Unique	
FMT_MTD.1/TOE_State	OT.Lifecycle_Management	

Table 13 SFRs and Security Objectives

Dependencies

10.3.3.1 SFRs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
FCS_RNG.1	No Dependencies	
FMT_MTD.1/TOE_State	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Unblock	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FPT_EMS.1	No Dependencies	
FPT_FLS.1	No Dependencies	
FPT_PHP.1	No Dependencies	
FPT_PHP.3	No Dependencies	
FPT_TST.1	No Dependencies	
FMT_SMR.1	(FIA_UID.1)	FIA_UID.1
FMT_SMF.1	No Dependencies	
FMT_MOF.1	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FMT_MSA.1/Admin	(FDP_ACC.1 or FDP_IFC.1) and (FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1, FDP_ACC.1/Signature_Creation, FDP_ACC.1/SVD_Transfer, FDP_ACC.1/SCD/SVD_Generation, FDP_ACC.1/SCD_Import
FMT_MSA.1/Signatory	(FDP_ACC.1 or FDP_IFC.1) and	FMT_SMR.1, FMT_SMF.1, FDP_ACC.1/Signature_Creation

	(FMT_SMF.1) and (FMT_SMR.1)	
FMT_MSA.2	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FDP_ACC.1/Signature_Creation, FDP_ACC.1/SCD/SVD_Generation
FMT_MSA.3	(FMT_MSA.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory
FMT_MSA.4	(FDP_ACC.1 or FDP_IFC.1)	FDP_ACC.1/Signature_Creation, FDP_ACC.1/SCD/SVD_Generation
FMT_MTD.1/Admin	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FMT_MTD.1/Signatory	(FMT_SMF.1) and (FMT_SMR.1)	FMT_SMR.1, FMT_SMF.1
FIA_UID.1	No Dependencies	
FIA_AFL.1	(FIA_UAU.1)	FIA_UAU.1
FIA_UAU.1	(FIA_UID.1)	FIA_UID.1
FDP_SDI.2/DTBS	No Dependencies	
FDP_SDI.2/Persistent	No Dependencies	
FDP_RIP.1	No Dependencies	
FDP_ACC.1/Signature_Creation	(FDP_ACF.1)	FDP_ACF.1/Signature_Creation
FDP_ACF.1/Signature_Creation	(FDP_ACC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/Signature_Creation
FCS_COP.1	(FCS_CKM.1 or FCS_CKM.5 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.6, FCS_CKM.1, FDP_ITC.1/SCD
FCS_CKM.6	(FCS_CKM.1 or FCS_CKM.5 or FDP_ITC.1 or FDP_ITC.2)	FCS_CKM.1, FDP_ITC.1/SCD
FCS_CKM.1	(FCS_CKM.2 or FCS_CKM.5 or FCS_COP.1) and (FCS_CKM.3) and (FCS_CKM.6) and (FCS_RBG.1 or FCS_RNG.1)	FCS_COP.1, FCS_CKM.6, FCS_RNG *FCS_CKM.3: discarded – No Key Access Interface exists*
FDP_ACC.1/SVD_Transfer	(FDP_ACF.1)	FDP_ACF.1/SVD_Transfer
FDP_ACF.1/SVD_Transfer	(FDP_ACC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/SVD_Transfer
FDP_ACC.1/SCD/SVD_Generation	(FDP_ACF.1)	FDP_ACF.1/SCD/SVD_Generation

FDP_ACF.1/SCD/SVD_Generation	(FDP_ACC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/SCD/SVD_Generation
FTP_ITC.1/SCD	No Dependencies	
FDP_UCT.1/SCD	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FTP_ITC.1/SCD, FDP_ACC.1/SCD_Import
FDP_ITC.1/SCD	(FDP_ACC.1 or FDP_IFC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/SCD_Import
FDP_ACC.1/SCD_Import	(FDP_ACF.1)	FDP_ACF.1/SCD_Import
FDP_ACF.1/SCD_Import	(FDP_ACC.1) and (FMT_MSA.3)	FMT_MSA.3, FDP_ACC.1/SCD_Import
FDP_UIT.1/DTBS	(FDP_ACC.1 or FDP_IFC.1) and (FTP_ITC.1 or FTP_TRP.1)	FDP_ACC.1/Signature_Creation, FTP_ITC.1/DTBS
FTP_ITC.1/DTBS	No Dependencies	

Table 14 SFRs Dependencies

Rationale for the exclusion of Dependencies

The dependency FMT_MSA.3 of FDP_ACF.1/TRM is discarded. The access control TSF according to FDP_ACF.1/TRM uses security attributes that have been defined during personalization, and that are fixed over the whole life time of the TOE. No management of these security attributes (i.e. SFR FMT_MSA.1 and FMT_MSA.3) is necessary.

10.3.3.2 SARs Dependencies

Requirements	CC Dependencies	Satisfied Dependencies
ADV_ARC.1	(ADV_FSP.1) and (ADV_TDS.1)	ADV_FSP.4, ADV_TDS.4
ADV_FSP.4	(ADV_IMP.1) and (ADV_TDS.1)	ADV_IMP.1, ADV_TDS.4
ADV_IMP.1	(ADV_TDS.3) and (ALC_TAT.1)	ADV_TDS.4, ALC_TAT.1
ADV_TDS.4	(ADV_FSP.5)	ADV_FSP.4
ADV_INT.2	(ADV_IMP.1) and (ADV_TDS.3) and (ALC_TAT.1)	ADV_IMP.1, ADV_TDS.4, ALC_TAT.1
AGD_OPE.1	(ADV_FSP.1)	ADV_FSP.4
AGD_PRE.1	No Dependencies	
ALC_CMC.4	(ALC_CMS.1) and (ALC_DVS.1) and (ALC_LCD.1)	ALC_CMS.4, ALC_DVS.2, ALC_LCD.1
ALC_CMS.4	No Dependencies	
ALC_DEL.1	No Dependencies	
ALC_DVS.2	No Dependencies	

ALC_FLR.3	No Dependencies	
ALC_LCD.1	No Dependencies	
ALC_TAT.1	(ADV_IMP.1)	ADV_IMP.1
ASE_CCL.1	(ASE_ECD.1) and (ASE_INT.1) and (ASE_REQ.1)	ASE_ECD.1, ASE_INT.1, ASE_REQ.2
ASE_ECD.1	No Dependencies	
ASE_INT.1	No Dependencies	
ASE_OBJ.2	(ASE_SPD.1)	ASE_SPD.1
ASE_REQ.2	(ASE_ECD.1) and (ASE_OBJ.2)	ASE_ECD.1, ASE_OBJ.2
ASE_SPD.1	No Dependencies	
ASE_TSS.1	(ADV_FSP.1) and (ASE_INT.1) and (ASE_REQ.1)	ADV_FSP.4, ASE_INT.1, ASE_REQ.2
ATE_COV.2	(ADV_FSP.2) and (ATE_FUN.1)	ADV_FSP.4, ATE_FUN.1
ATE_DPT.1	(ADV_ARC.1) and (ADV_TDS.4) and (ATE_FUN.1)	ADV_ARC.1, ADV_TDS.4, ATE_FUN.1
ATE_FUN.1	(ATE_COV.1)	ATE_COV.2
ATE_IND.2	(ADV_FSP.2) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_COV.1) and (ATE_FUN.1)	ADV_FSP.4, AGD_OPE.1, AGD_PRE.1, ATE_COV.2, ATE_FUN.1
AVA_VAN.5	(ADV_ARC.1) and (ADV_FSP.4) and (ADV_IMP.1) and (ADV_TDS.3) and (AGD_OPE.1) and (AGD_PRE.1) and (ATE_DPT.1)	ADV_ARC.1, ADV_FSP.4, ADV_IMP.1, ADV_TDS.4, AGD_OPE.1, AGD_PRE.1, ATE_DPT.1

Table 15 SARs Dependencies

10.3.4 Rationale for the Security Assurance Requirements

The assurance level for this Security Target is EAL4 augmented. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialized processes and practices. It is considered to be the highest level that could be applied to an existing product line without undue expense and complexity. As such, EAL4 is appropriate for commercial products that can be applied to moderate to high security functions. Augmentation results from the selection of:

AVA_VAN.5 Advanced methodical vulnerability analysis ALC_DVS.2 Sufficiency of security measures ALC_FLR.3 Systematic flaw remediation

10.3.5 AVA_VAN.5 Advanced methodical vulnerability analysis

The TOE is intended to function in a variety of signature creation systems for qualified electronic signatures. Due to the nature of its intended application, i.e., the TOE may be issued to users and may not be directly under the control of trained and dedicated administrators. As a result, it is imperative that misleading, unreasonable and conflicting guidance is absent from the guidance documentation, and that secure procedures for all modes of operation have been addressed. Insecure states should be easy to detect. The TOE shall be shown to be highly

resistant to penetration attacks to meet the security objectives OT.SCD_Secrecy, OT.Sigy_SigF and OT.Sig_Secure.

10.3.6 ALC_DVS.2 Sufficiency of security measures

Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE. Due to the nature of the TOE, there is a need to justify the sufficiency of these procedures to protect the confidentiality and the integrity of the TOE. The TOE shall be protected in confidentiality and integrity during its development to meet the security objective OT.Lifecycle_Security.

10.3.7 ALC_FLR.3 systematic flaw remediation

ALC_FLR.3 provides assurance to the users that IDEMIA has policies and procedures to track and correct flaws, and to distribute the flaw information and corrections.

11 TOE Summary Specification

11.1 TOE Summary Specification

This section provides a summary of the security functions implemented by the TOE in order to fulfil the security functional requirements. The summary is structured in security functions.

The security functionalities concerning the IC and the JC Platform are described in [ST-IC], [ST-PL] and are not redefined in this security target, although they must be considered for the TOE.

11.1.1 Chip security functionalities

The full list of the IC Platform security functionalities can be checked in the IC Platform Security Target [ST-IC].

11.1.2 Platform security functionalities

The full list of the JC Platform security functionalities can be checked in the JC Platform Security Target [ST-PL].

11.1.3 Application security functionalities

SF.AUTHENTICATION

Only authenticated terminals can get access to the user data stored on the TOE. The MobileID Applet offers several authentication schemes enabling to authenticate different roles, such as:

- The signatory entitled to use the services offered by the card. It is called "User Authentication".
- The device communicating with the card, to establish a trusted channel (secure messaging) and protect the communication. It is called "Device authentication".
- The administrator of a service, to administrate some features. It is called "Role authentication".

The **User authentication** is based on the submission of a PIN/password.

- Knowledge based: The Authentication of the user relies on a shared secret (PIN), known by both the holder and the smartcard. The Card holder is authenticated by the means of the VERIFY command. For each SCD separate signatory's RADs (PINs) are assigned. The verification process uses a velocity checking mechanism, thus a remaining tries counter and a maximum error counter are defined for each PIN. If the verification fails, the tries counter is decremented by one and an error status that contains the remaining attempts is returned by the application. When all available tries have failed, the PIN is blocked and can no longer be used. Note that a successful verification of the PIN resets its remaining tries counter to the maximum error counter.

The **Device Authentication** aims at authenticating both entities willing to communicate and securing the communication between the card and a service provider (it might be a terminal, a server, etc).

- Authentication Scheme: The smart card implements a mutual authentication scheme. This one relies either on AES Cipher block and used to:
  - Authenticate the terminal and the card.

- Generate two temporary keys that will be further used to compute session keys for the secure messaging in the subsequent commands.
- Initialize the counter used at each checksum computation.

The **Role Authentication** presents the procedure to authenticate an external entity to the card in order to associate to it a specific role (e.g. access rights). Schemes may be used, relying either AES. The following procedure describes:

- The cryptographic operation that allows the authentication
- The specification of the associated role in the card This feature is described in [TR_SIG]. In MobileID, the Access conditions "Secure Messaging" mandates both a successful terminal authentication and an active secure messaging session. This security function manages authentication failure: when the "highest value in the configurable range of positive numbers fixed by the Administrator" unsuccessful authentication attempts have been met, the TSF shall block the RAD. This security functionality allows the following operations to be performed before the user is authenticated:
- Identification of the user,
- Establishing a trusted channel between the SCA and the TOE,
- Establishing a trusted channel between the CGA and the TOE.

The OS implements all the cryptographic operations and the TOE uses them.

SF.APP_CRYPTO

This SF performs high level cryptographic operations: The OS implements all the cryptographic algorithms or key generation and the TOE uses them for:

- key generation:
  - SF.APP_CRYPTO performs Elliptic curves key generation of size 256 bits in conformance with ANS X9.62.
- Digital signature generation:
  - the signature generation function shall have an access condition based upon previous authentication of user.
  - signature generation by using ECDSA algorithm with cryptographic key sizes of 256 bits (provided by the cryptographic library of the Platform).
- SCD/SVD key pair consistency check: SF.APP_CRYPTO performs SCD/SVD consistency check before signature generation by signature generation followed by signature verification. If the signature verification does not match the signature generation, then the key pair is not consistent.
- Secure messaging (encryption and decryption) using:
  - AES in CBC mode (key sizes 128,192,256 bits).
- Secure messaging (message authentication code) using:
  - AES CMAC with key sizes 128,192 and 256 bits.
- Authentication cryptogram creation/verification: SF.APP_CRYPTO performs the following authentication cryptogram calculation/verification:
  - Mutual authentication based AES
- Random number generation that meet FCS_RNG.1 Quality metric for random numbers of [ST-PL].
- Symmetric Role Authentication using AES
- Symmetric Device Authentication using AES
- Data Hashing: SF.APP_CRYPTO performs SHA-1, SHA2-256, SHA2-384, SHA2-512 in conformance with NIST FIPS PUB 180-3, in order to calculate a hash value.

- GP Secret data encryption using SCP03.
- Symmetric Encryption and Decryption using AES-CBC mode with key sizes 128, 192, 256 bits

All cryptographic functionalities are provided by the platform (see [ST-PL].

SF.MANAGEMENT

This SF manages the access to objects (files, directories, data and secrets) stored in the MobileID file system. It also controls write access of initialization and personalization data. This SF ensures secure management of secrets such as cryptographic keys. It also covers access to keys as well as secure key deletion. This SF controls all the operations relative to the RAD/VAD management, including the Cardholder (signatory) authentication:

- RAD creation: the RAD is stored and is associated to a maximum successful presentation number (usage counter) and to a maximum error number.
- VAD verification: the RAD can be accessed only if its format and integrity are correct and if the usage counter has not reached 0. If the RAD is blocked, then it cannot be used anymore until unblocked.
- RAD ratification counter: The number of authentication attempts is limited by a counter associated to the RAD. The counter is decremented each time the VAD verification fails. The RAD cannot be used any longer if the counter reaches zero.
- RAD usage counter: the usage counter is decremented each time the RAD is verified successfully. When this counter reaches 0, the RAD cannot be verified anymore.
- RAD modification: the RAD can be changed by the cardholder (loading a new value). The RAD is managed and stored by the application. The operations on RAD and VAD are performed thanks to services offered by the platform.

This SF manages the security environment of the application and:

- Maintains the roles (e.g. Signatory and Administrator).
- Controls if the authentication required for a specific operation has been performed with success.
- Manages restriction to security function access and to security attribute modification.
- Ensures that only secure values are accepted for security attributes. This security functionality restricts the ability to perform the function Signature creation SFP to Signatory. This security functionality ensures that only Administrator is authorized to
  - Modify Initialization SFP and Signature creation SFP attributes
  - Specify alternative default values

This SF provides the electronic signature application with access control and ensures that the following operations are executed by authorized roles:

- Export of SVD to CGA
- Generation of SCD/SVD pair by the Signatory
- Creation of RAD by the Administrator
- Signing of DTBS/R by S.Signatory

This SF manages Session key generation: Session keys are protected in integrity and confidentiality during generation. This SF enforces secure storage of the session keys during generation. This SF manages Secret destruction: This SF calls the security function of the JC Platform to erase keys. The applet mobileID uses this cryptographic key generation algorithm but it is implemented by the OS.

This SF manages Secret loading: Loading of a secret is always done by an authorized user through a secure command. This command is accepted only after authentication of the authorized user.

This SF manages Secret transfer: This SF manages the secure transfer of every secret to the crypto processor when used for cryptographic operation. Access control is enforced by the APDU or SMS methods as specified in the interface defined in the functional specification.

SF.TRUSTED_CHANNEL

This SF realizes a secure communication channel to verify authenticity and integrity as well as securing confidentiality of user data between the TOE and other devices connected.

The MobileID Package performs the following secure messaging tasks with external applications (SCA or CGA) for protection of the communication data as the DTBS or for ensuring the integrity of the SVD:

The OS implements all the cryptographic algorithms and the TOE uses them for:

- Encryption and decryption of the transmitted message.
- MAC generation and verification for secure messaging.
- Secure hash computation.
- Random number generation.

This SF manages four modes of secure channel during the personalization phase:

- No secure messaging
- Integrity mode
- Confidentiality mode
- Integrity and confidentiality mode

SF.APP_INTEGRITY

This security functionality monitors the integrity of sensitive user data and the integrity of the DTBS/R. The integrity of persistently stored data such as SCD, RAD and SVD is monitored using the platform features (see [ST-PL])). In case of integrity error this TSF will:

- Prohibit the use of the altered data, and
- Inform the S.Signatory about integrity error. This TSF also monitors the integrity of the access conditions of created data objects and also ensures that no residual information is available after a RAD update or clearance.

SF.RATIF

A counter is associated to a secret key, to a password and to the VAD, which is used to count the number of successive unsuccessful authentication attempts. The counter is reinitialized when the authentication is successful. If the counter reaches its maximum value, then the related secret is suspended or blocked and cannot be used anymore.

SF.ESERVICE

This security function enables to perform electronic services. It is active in phase 7. This security function offers the following electronic services:

- C/S authentication
- Symmetric encryption and decryption

SF.ADM_AUTH

This security function manages the authentication of external entities by the TOE. It is active in phase 6 and 7. This security function enables the TOE to authenticate external entities and may be either realized using symmetric or asymmetric cryptography. This security function manages as well the validation process of the role associated to the authentication key used by the external entity. Upon successful authentication, the associated role is authenticated and can proceed to switch from Phase 6 to Phase 7 for example. Each key is associated to an error counter (it may be infinite) which aims at ensuring its protecting against brute force attacks. Upon each wrong authentication, it decrements the error counter (if present) and restores it to its maximum value upon successful authentication. When the error counter has reached '00', the security function blocks the usage of the key, and bans the authentication of the associated role. This security function allows the authentication of the following roles:

- R.Admin

11.2 SFRs and TSS

11.2.1 SFRs and TSS - Rationale

All SSCD parts

Protection of the TSF (FPT)

FPT_EMS.1 is met by SF.APP_INTEGRITY and SF.MANAGEMENT which ensure secure execution of cryptographic operations on keys.

FPT_FLS.1 is met by JC Platform and the IC that ensure that failures in the TSF are detected and that the proper actions (reset, card termination) are taken in order to preserve a secure sate of the TOE. It is also met by SF.APP_INTEGRITY that monitors the integrity of sensitive user data and the integrity of the DTBS/R.

FPT_PHP.1 is met by SF.APP_INTEGRITY, the JC Platform and the IC that ensure that physical tampering of the TOE is detected and that the proper actions (reset, card termination) are taken, so that is can be determined if a physical tampering has occurred.

FPT_PHP.3 is met by the JC Platform and the IC that ensures that physical tampering of the TOE is detected and that the proper actions (reset, card termination) in order to protect the TOE.It is also met by SF.APP_INTEGRITY that monitors the integrity of sensitive data.

FPT_TST.1 is met by JC Platform and the IC that performs a set of self-tests at start-up, thus checking the correct operation of the TSF, and that verifies the integrity of the stored

executable code before or during its execution and by SF.APP_INTEGRITY that provides means to verify the integrity of the data stored on the TOE.

Security management (FMT)

FMT_SMR.1 is met by SF.AUTHENTICATION that provides user authentication as administrator or as signatory and by SF.MANAGEMENT that grants to the administrator and to the signatory specific access rights, thus defining roles for the TOE.

FMT_SMF.1 requires that the TSF shall be capable of performing the following management functions: (1) Creation and modification of the reference authentication data (RAD), (2) Enabling the signature-creation function, (3) Modification of the security attribute SCD/SVD management, SCD operational, (4) Change the default value of the security attribute SCD Identifier, (5) none. This is realized by SF.MANAGEMENT.

FMT_MOF.1 is met by SF.MANAGEMENT and SF.AUTHENTICATION that ensures that only authenticated signatory can perform DTBS signature.

FMT_MSA.1/Admin is met by SF.AUTHENTICATION and SF.MANAGEMENT that manage the access right policy of the TOE.

FMT_MSA.1/Signatory is met by SF.AUTHENTICATION and SF.MANAGEMENT that manage the access right policy of the TOE.

FMT_MSA.2 is met by SF.AUTHENTICATION and SF.MANAGEMENT that manage the access right policy of the TOE and in particular manages the security attributes.

FMT_MSA.3 is met by SF.AUTHENTICATION and SF.MANAGEMENT that manage the access right policy of the TOE and in particular manage the security attributes, their initialisation and their access rights.

FMT_MSA.4 requires that the TSF shall use the following rules to set the value of security attributes: (1) if S.Admin successfully generates an SCD/SVD pair without S.Sigy being authenticated the security attribute 'SCD operational of the SCD' shall be set to 'no' as a single operation; (2) if S.Sigy successfully generates an SCD/SVD pair the security attribute 'SCD operational of the SCD' shall be set to 'yes' as a single operation. This is realized by SF.MANAGEMENT and SF.AUTHENTICATION.

FMT_MTD.1/Admin

- is met by SF.MANAGEMENT that manages the authentication function and ensure that only authenticated administrator can create the RAD.
- is met by SF.AUTHENTICATION that provides the authentication protocol.

FMT_MTD.1/Signatory

- is met by SF.MANAGEMENT that manages the authentication function and ensure that only authenticated signatory can modify the RAD.
- is met by SF.AUTHENTICATION that provides the authentication protocol.

Identification and authentication (FIA)

FIA_UID.1

- is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.

FIA_AFL.1

- This SFR is met by SF.AUTHENTICATION and SF.MANAGEMENT.
- This SFR is also met by SF.RATIF that ensures that the RAD is blocked after a defined number of failed successive signatory authentication attempts.

FIA_UAU.1

- is met by SF.AUTHENTICATION and SF.MANAGEMENT that provide user identification and user authentication prior to enabling access to authorized functions.
- is met by SF.TRUSTED_CHANNEL that provides a trusted secure messaging with CGA and SCA.

User data protection (FDP)

FDP_SDI.2/DTBS is met by SF.APP_INTEGRITY, that ensures the integrity of data stored in the TOE, by the JC Platform and the IC that ensure that the proper reaction is taken (reset or card termination) if an integrity error is detected, so that the user knows an error had occurred and that no altered data can be used.

FDP_SDI.2/Persistent is met by SF.APP_INTEGRITY, that ensures the integrity of data stored in the TOE, by the JC Platform and the IC that ensure that the proper reaction is taken (reset or card termination) if an integrity error is detected, so that the user knows an error had occurred and that no altered data can be used.

FDP_RIP.1 is met by SF.MANAGEMENT that ensures erasure of data in FLASH and in RAM (e.g. after the signature creation process), and in particular of SCD, VAD and RAD.

FDP_ACC.1/Signature_Creation is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that all the access conditions are met before a dedicated operation can be performed, and in particular that only a user authenticated as signatory can perform signature of DTBS loading from an authorized SCA with a ECC key pair whose consistency has been verified, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACF.1/Signature_Creation is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that all the access conditions are met before a dedicated operation can be performed, and in particular that only a user authenticated as signatory can perform signature of DTBS loading from an authorized SCA with a Ecc key pair whose consistency

has been verified, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

Cryptographic support (FCS)

FCS_COP.1

- is met by SF.APP_CRYPTO that provides ECC key pair consistency check.
- is met by SF.APP_CRYPTO that provides electronic signature generation compliant with ECC ANS X9.62.
- is met by SF.APP_CRYPTO that provides AES in CBC mode for encryption and decryption.
- is met by SF.APP_CRYPTO that provides ISO/IEC 9797-1 Method 2 padding CMAC (AES) for integrity.
- is met by SF.AUTHENTICATION that provides Symmetric and Asymmetric Mutual Authentications.
- is met by SF.TRUSTED_CHANNEL that provides secure messaging with CGA and SCA.
- is met by SF.APP_CRYPTO that provides Data Hashing.
- is met by SF.APP_CRYPTO that provides signtaure verification.
- is met by SF.APP_CRYPTO that provides AES in CBC mode for encryption and decryption.
- is met by SF.TRUSTED_CHANNEL that provides secure messaging with CGA and SCA.
- is met by SF.APP_CRYPTO that provides AES in CBC mode for MAC calculation.
- is met by SF.TRUSTED_CHANNEL that provides secure messaging with CGA and SCA.

FCS_CKM.6 is met by SF.MANAGEMENT, as SF.MANAGEMENT manages the secure destruction of secret, and in particular of the SCD.

SSCD parts 2, 3 and addition from 5 only

Cryptographic support (FCS)

FCS_CKM.1

- is met by SF.APP_CRYPTO that ensures that the TOE generates SCD/SVD cryptographic key pairs.
- is also met by SF.MANAGEMENT, which ensures the protection of the keys during generation.

User data protection (FDP)

FDP_ACC.1/SVD_Transfer is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SVD export, and by

SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACF.1/SVD_Transfer is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SVD export, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACC.1/SCD/SVD_Generation is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user under specific conditions can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SCD/SVD generation, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACF.1/SCD/SVD_Generation is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user under specific conditions can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SCD/SVD generation, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

SSCD parts 3 only

Trusted path/channels (FTP)

FTP_ITC.1/SCD is met by SF.AUTHENTICATION and SF.MANAGEMENT that enforce the access right policy for SCD Import and by SF.TRUSTED_CHANNEL, SF.APP_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and a CSP to protect the exchanged data (SCD) from modification and disclosure.

User data protection (FDP)

FDP_UCT.1/SCD is met by SF.AUTHENTICATION and SF.MANAGEMENT that ensure that all the conditions are met before allowing a SCD import and by SF.TRUSTED_CHANNEL, SF.APP_CRYPTO that provide cryptographic means to protect the SCD from disclosure during its import.

FDP_ITC.1/SCD is met by SF.AUTHENTICATION and SF.MANAGEMENT that ensure that all the required conditions are met before allowing a SCD import operation.

FDP_ACC.1/SCD_Import is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SCD import, and by SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

FDP_ACF.1/SCD_Import is met by SF.MANAGEMENT, SF.AUTHENTICATION that ensure that only an authorized user can perform a dedicated operation, and in particular that only users authenticated as administrator or signatory can perform SCD import, and by

SF.MANAGEMENT, which verify that each received command security status is consistent with the security status of the TOE.

Additions from SSCD parts 5 only

User data protection (FDP)

FDP_UIT.1/DTBS requires that integrity of the DTBS/R to be signed is to be verified, as well as the DTBS/R is not altered by the TOE. This is provided by the trusted channel integrity verification mechanisms (SF.TRUSTED_CHANNEL, SF.APP_CRYPTO).

Trusted path/channels (FTP)

FTP_ITC.1/DTBS is met by SF.AUTHENTICATION and SF.MANAGEMENT that enforce the access right policy for DTBS Import and by SF.TRUSTED_CHANNEL, SF.APP_CRYPTO that provide cryptographic means to set up a trusted channel between the TOE and a SCA to protect the exchanged data (DTBS) from modification and disclosure.

Additional SFRs

FCS_RNG.1

- is met by SF.APP_CRYPTO and SF.AUTHENTICATION.

FMT_MTD.1/TOE_State is met by SF.ADM_AUTH that manages the authentication function and ensures that only authenticated by GP authentication in phase 6 (personalizer) can switch the life cycle. This last operation is ensured by the SF.MANAGEMENT.

11.2.2 Association tables of SFRs and TSS

Security Functional Requirements	TOE Summary Specification
FPT_EMS.1	SF.APP_INTEGRITY, SF.MANAGEMENT
FPT_FLS.1	SF.APP_INTEGRITY
FPT_PHP.1	SF.APP_INTEGRITY
FPT_PHP.3	SF.APP_INTEGRITY
FPT_TST.1	SF.APP_INTEGRITY
FMT_SMR.1	SF.AUTHENTICATION, SF.MANAGEMENT
FMT_SMF.1	SF.MANAGEMENT
FMT_MOF.1	SF.MANAGEMENT, SF.AUTHENTICATION
FMT_MSA.1/Admin	SF.MANAGEMENT, SF.AUTHENTICATION
FMT_MSA.1/Signatory	SF.MANAGEMENT, SF.AUTHENTICATION
FMT_MSA.2	SF.MANAGEMENT, SF.AUTHENTICATION
FMT_MSA.3	SF.MANAGEMENT, SF.AUTHENTICATION
FMT_MSA.4	SF.MANAGEMENT, SF.AUTHENTICATION
FMT_MTD.1/Admin	SF.MANAGEMENT, SF.AUTHENTICATION

FMT_MTD.1/Signatory	SF.MANAGEMENT, SF.AUTHENTICATION
FIA_UID.1	SF.AUTHENTICATION, SF.MANAGEMENT
FIA_AFL.1	SF.MANAGEMENT, SF.AUTHENTICATION, SF.RATIF
FIA_UAU.1	SF.AUTHENTICATION, SF.MANAGEMENT, SF.TRUSTED_CHANNEL
FDP_SDI.2/DTBS	SF.APP_INTEGRITY
FDP_SDI.2/Persistent	SF.APP_INTEGRITY
FDP_RIP.1	SF.MANAGEMENT
FDP_ACC.1/Signature_Creation	SF.MANAGEMENT, SF.AUTHENTICATION
FDP_ACF.1/Signature_Creation	SF.MANAGEMENT, SF.AUTHENTICATION
FCS_COP.1	SF.APP_CRYPTO, SF.AUTHENTICATION, SF.TRUSTED_CHANNEL
FCS_CKM.6	SF.MANAGEMENT
FCS_CKM.1	SF.APP_CRYPTO, SF.MANAGEMENT
FDP_ACC.1/SVD_Transfer	SF.MANAGEMENT, SF.AUTHENTICATION
FDP_ACF.1/SVD_Transfer	SF.MANAGEMENT, SF.AUTHENTICATION
FDP_ACC.1/SCD/SVD_Generation	SF.MANAGEMENT, SF.AUTHENTICATION
FDP_ACF.1/SCD/SVD_Generation	SF.MANAGEMENT, SF.AUTHENTICATION
FTP_ITC.1/SCD	SF.MANAGEMENT, SF.APP_CRYPTO, SF.TRUSTED_CHANNEL, SF.AUTHENTICATION
FDP_UCT.1/SCD	SF.TRUSTED_CHANNEL, SF.APP_CRYPTO, SF.AUTHENTICATION, SF.MANAGEMENT
FDP_ITC.1/SCD	SF.MANAGEMENT, SF.AUTHENTICATION
FDP_ACC.1/SCD_Import	SF.MANAGEMENT, SF.AUTHENTICATION
FDP_ACF.1/SCD_Import	SF.MANAGEMENT, SF.AUTHENTICATION
FDP_UIT.1/DTBS	SF.TRUSTED_CHANNEL, SF.APP_CRYPTO
FTP_ITC.1/DTBS	SF.TRUSTED_CHANNEL, SF.APP_CRYPTO, SF.MANAGEMENT, SF.AUTHENTICATION
FCS_RNG.1	SF.APP_CRYPTO, SF.AUTHENTICATION
FMT_MTD.1/TOE_State	SF.MANAGEMENT, SF.ADM_AUTH

Table 16 SFRs and TSS - Coverage

TOE Summary Specification	Security Functional Requirements
SF.AUTHENTICATION	FMT_SMR.1, FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory, FIA_UID.1, FIA_AFL.1, FIA_UAU.1, FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation, FCS_COP.1, FDP_ACC.1/SVD_Transfer, FDP_ACF.1/SVD_Transfer, FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FTP_ITC.1/SCD, FDP_UCT.1/SCD, FDP_ITC.1/SCD, FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import, FTP_ITC.1/DTBS
SF.APP_CRYPTO	FCS_COP.1, FCS_CKM.1, FTP_ITC.1/SCD, FDP_UCT.1/SCD, FDP_UIT.1/DTBS, FTP_ITC.1/DTBS
SF.MANAGEMENT	FMT_MTD.1/TOE_State , FPT_EMS.1, FMT_SMR.1, FMT_SMF.1, FMT_MOF.1, FMT_MSA.1/Admin, FMT_MSA.1/Signatory, FMT_MSA.2, FMT_MSA.3, FMT_MSA.4, FMT_MTD.1/Admin, FMT_MTD.1/Signatory, FIA_UID.1, FIA_AFL.1, FIA_UAU.1, FDP_RIP.1, FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation, FCS_CKM.6, FCS_CKM.1, FDP_ACC.1/SVD_Transfer, FDP_ACF.1/SVD_Transfer, FDP_ACC.1/SCD/SVD_Generation, FDP_ACF.1/SCD/SVD_Generation, FTP_ITC.1/SCD, FDP_UCT.1/SCD, FDP_ITC.1/SCD, FDP_ACC.1/SCD_Import, FDP_ACF.1/SCD_Import, FTP_ITC.1/DTBS
SF.TRUSTED_CHANNEL	FIA_UAU.1, FCS_COP.1, FTP_ITC.1/SCD, FDP_UCT.1/SCD, tok273FDP_UIT.1/DTBS, FTP_ITC.1/DTBS
SF.APP_INTEGRITY	FPT_EMS.1, FPT_FLS.1, FPT_PHP.1, FPT_PHP.3, FPT_TST.1, FDP_SDI.2/DTBS, FDP_SDI.2/Persistent
SF.RATIF	FIA_AFL.1
SF.ADM_AUTH	FMT_MTD.1/TOE_State

Table 17 TSS and SFRs - Coverage