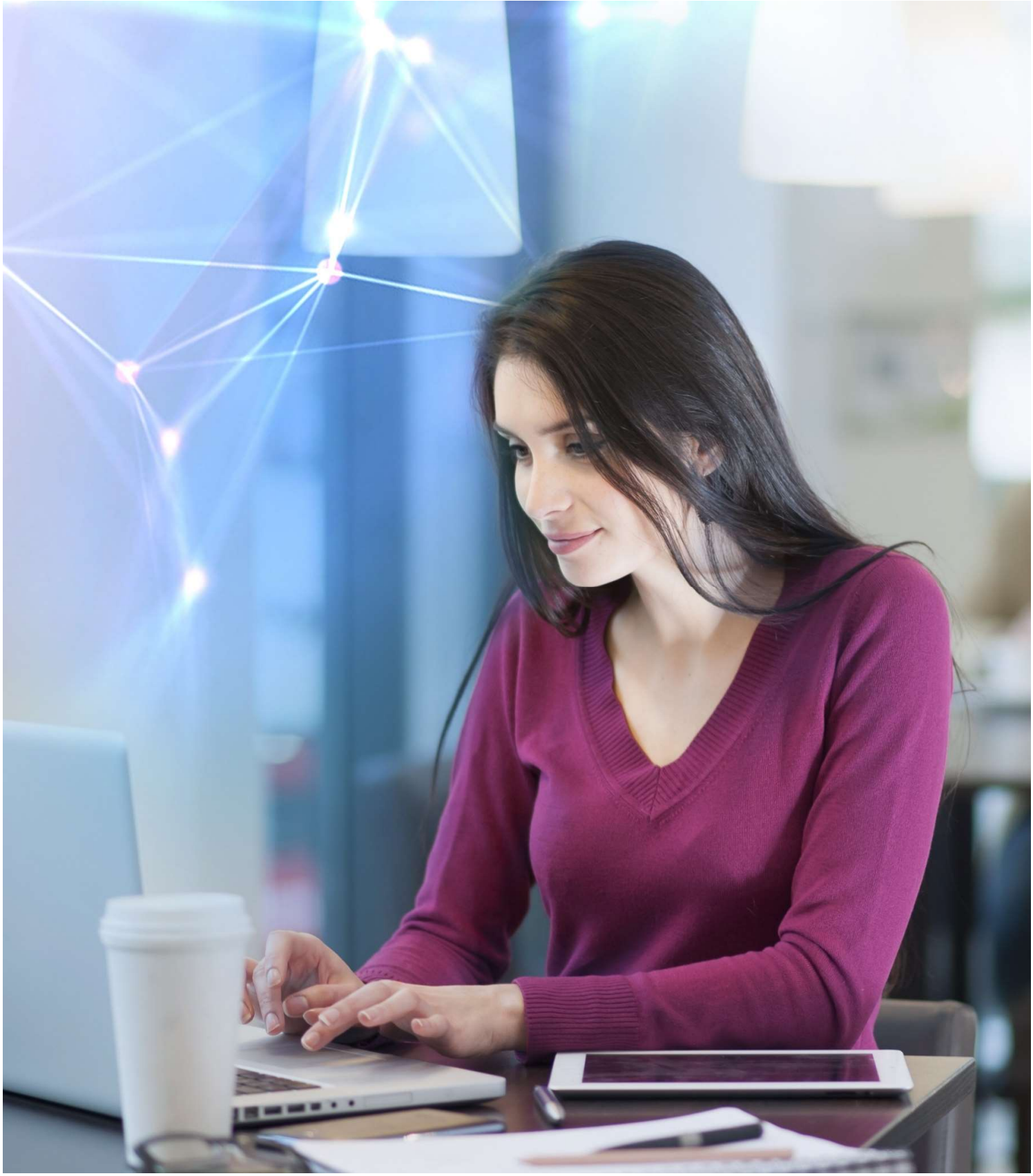

SafeSign IC on JCOP 4 P71

Security Target

Table of contents

Warning Notice

All information herein is either public information or is the property of and owned solely by A.E.T. Europe B.V. who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Installation and use of A.E.T. Europe B.V. products are subject to your acceptance of the terms and conditions set out in the license Agreement that accompanies each product. Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/ or industrial property rights of or concerning any of A.E.T. Europe B.V. information.

Cryptographic products are subject to export and import restrictions. You are required to obtain the appropriate government licenses prior to shipping this Product.

Document Information

Document ID:

Project Information:

Document revision history:

Version	Date	Author	Changes
1.0	14 Jun 2019	Arjan Jeckmans	Initial version for release
1.1	21 Aug 2020	Arjan Jeckmans	Update to JCOP 4 P71
1.2	8 Oct 2020	Arjan Jeckmans	Updated references
1.3	4 Dec 2020	Arjan Jeckmans	Updated PP references, TOE overview, and table 1
1.4	9 Mar 2021	Arjan Jeckmans	Updated to latest JCOP 4 P71 certification
1.5	12 Apr 2021	Arjan Jeckmans	Updated guidance references

About the Product

SafeSign Identity Client (IC) is a software package that can be used to enhance the security of applications that support hardware tokens through PKCS #11 and Microsoft CryptoAPI.

The SafeSign IC package provides a standards-based PKCS #11 Library as well as a Cryptographic Service Provider (CSP) and CNG Key Storage Provider (KSP) allowing users to store public and private data on a personal token, either a smart card, USB token or SIM card. It also includes the SafeSign IC PKI applet, enabling end-users to utilise any Java Card 2.1.1 / Java Card 2.2 and higher compliant card with the SafeSign IC middleware.

Combining full compliance with leading industry standards and protocols, with flexibility and usability, SafeSign IC can be used with multiple smart cards / USB tokens, multiple Operating Systems and multiple smart card readers.

SafeSign IC allows users to initialise and use the token for encryption, authentication or digital signatures and includes all functionality necessary to use hardware tokens in a variety of PKI environments.

SafeSign IC comes in a standard version with an installer for Windows, MAC and Linux environments. It is also available for many other environments like mobile devices.

For more information, refer to the latest SafeSign IC Product Description on www.aeteurope.com.

References

- BSI Cryptographic Mechanisms: Recommendations and Key Lengths v2020-01 (BSI TR-02102-1), 24-03-2020
- CC1 Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model v3.1r5 (CCMB-2017-04-001), 04-2017
- CC2 Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components v3.1r5 (CCMB-2017-04-002), 04-2017
- CC3 Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components v3.1r5 (CCMB-2017-04-003), 04-2017
- CEM Common Methodology for Information Technology Security Evaluation, Evaluation Methodology v3.1r5 (CCMB-2017-04-004), 04-2017
- EU 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, 23-07-2014
- FSP SafeSign IC PKI Applet v3 Interface Specification v3.4, generated with applet
- OPE Operational Guidance SafeSign IC eIDAS QSCD on JCOP 4 P71 v1.2, 12-04-2021
- PP2 EN-419211-2:2013 Protection profiles for secure signature creation device - Part 2: Device with key generation v2.0.1 (BSI-CC-PP-0059-2009-MA-02), 07-2013
- PP3 EN-419211-3:2013 Protection profiles for secure signature creation device - Part 3: Device with key import v1.0.2 (BSI-CC-PP-0075-2012-MA-01), 10-2013
- PRE Preparative Procedures SafeSign IC eIDAS QSCD on JCOP 4 P71 v1.2, 12-04-2021
- PST JCOP 4 P71 Security Target Lite v4.1, 12-02-2021

Abbreviated Terms

- **CGA** Certificate Generation Application
- **CSP** Certification Service Provider
- **DTBS** Data to be Signed
- **DTBS/R** Data to be Signed or its Unique Representation
- **eIDAS** Electronic Identification, Authentication and Trust Services
- **QSCD** Qualified Signature Creation Device
- **RAD** Reference Authentication Data
- **SCA** Signature Creation Application
- **SCD** Signature Creation Data
- **SSCD** Secure Signature Creation Device
- **SVD** Signature Verification Data
- **VAD** Verification Authentication Data

1 Introduction

1.1 ST and TOE Reference

ST Title: SafeSign IC PKI applet on JCOP 4 P71 eIDAS QSCD Security Target

ST Revision: v1.5

ST Date: 12 Apr 2021

ST Author: A.E.T. Europe B.V.

TOE Reference: SafeSign IC PKI applet on JCOP 4 P71 eIDAS QSCD v3.0.1.12

1.2 TOE Overview

The TOE, of type smart card, consists of a Java Card applet on top of an OS providing the Java Card and GlobalPlatform interface on top of a micro controller. The applet provides PKI and PKCS#15 functionality. The TOE provides the functionality of an eIDAS QSCD with protection of private key material and qualified certificates. In order for applications to communicate with the TOE, the appropriate middleware is required.

1.3 TOE Description

This TOE is a composite TOE consisting of a Java Card applet combined with the JCOP 4 P71 Java Card. The reference for this Java Card is as follows:

Reference: JCOP 4 P71

Certification ID: CC-21-180212

ST Reference: JCOP 4 P71 Security Target Lite, Revision 4.1, 2021-02-12 [PST]

This Java Card is also a composite, but its components are not listed here. Please refer to the security target lite for a complete overview of the JCOP 4 P71 components.

The TOE can be identified by issuing the following APDU command to the applet “0x00CA010304”, this should result in the following response “0x0300010C9000”. The Java Card can be identified by means detailed in section 1.3.4 of the JCOP 4 P71 Security Target Lite [PST].

1.3.1 Intended Usage

The TOE is intended to be used as a portable personal electronic signature creation device in a managed IT environment where the electronic signature is used as proof of authenticity and/or presence of the signatory. The TOE interacts with the environment by means of standard smart card interfaces.

The signatory is required to provide authentication information to the TOE before it creates an electronic signature, thereby preventing unauthorized use of the TOE.

The physical shape of the TOE is not defined here, although it is typically a smart card form factor and could carry printed information about the signatory.

1.3.2 TOE Boundary

The following diagram shows a simplified view of the components present in the composite TOE.

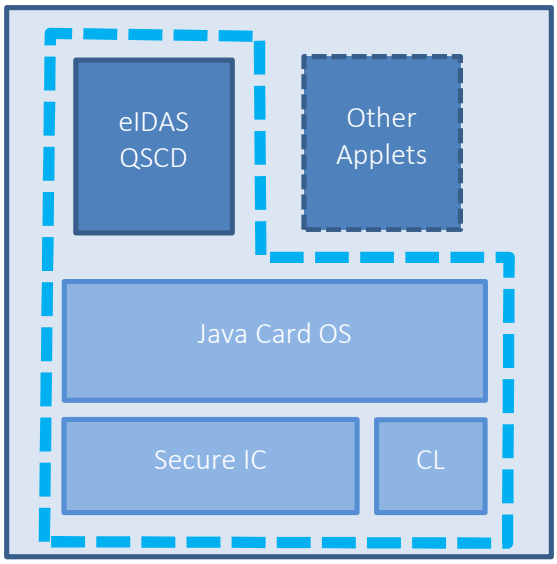

Figure 1. TOE components and boundary

The TOE boundary is indicated by the dashed line. In this boundary are:

- The Secure IC with cryptographic library (CL) combined with the Java Card OS, is the already certified component of the TOE.
- The SafeSign IC PKI applet eIDAS QSCD implementing the TSF.

The platform is defined as an open Java Card platform and other applications may be present on this platform. Such other applets are not part of the TOE and are placed outside the TOE boundary.

Note that as part of the production phase, the platform is transitioned to a closed Java Card platform. This means that other applets cannot be loaded and installed during the usage phase.

1.3.3 Other Required Hardware and Software

In order to use the TOE a standard smart card acceptance device is required, as well as software to allow the signatory and the other roles to interact with the TOE.

The software also provides integration of the TOE functionality for the operating system.

1.3.4 TOE Life Cycle

The TOE life cycle consists of 3 phases; development, production, and usage.

In the development phase the SafeSign IC PKI applet part of the TOE is developed, reviewed and tested. After development is completed, the applet is built and prepared for delivery. The development phase ends with the delivery of the delivery package (see the next section) to the TOE producer.

In the production phase the TOE is assembled and bound to a specific signatory. First the Java Card is prepared and the applet (loaded and) initialized. Second the Java Card is secured. Third, the TOE is personalized. The RAD (or a transport equivalent) for the signatory is defined and entered, key material (SCD/SVD) is either generated or imported, and certificates are loaded. Generally, the signatory is not present in this phase and keys are marked as non-operational.

Upon delivery, the signatory validates the TOE and activates the keys. Also the RAD can be set upon delivery if required (transport equivalent). With the delivery to the signatory the production phase ends.

In the usage phase the signatory can use the available SCD to produce signatures and possibly generate new SCD/SVD pairs. Keys generated and imported in this phase are automatically operational.

1.3.5 TOE Delivery

The TOE is not delivered as the final composite product. The applet can be either pre-loaded onto the platform, or delivered separately for loading during the production phase.

In case the applet is pre-loaded, the delivery consists of a binary archive containing:

- A container file containing the following elements:
  - The SafeSign IC PKI Applet v3 Interface Specification [FSP].
  - The test report of the applet.
  - An information file containing:
    - The used configuration.
    - The unique identifier of the toolchain versions.
    - The fingerprint of the used revision from all version control repositories.
    - The unique identifier of the applet.
- The preparative procedures document [PRE].
- The operational guidance document [OPE].

In case the applet is delivered separately, the delivery consists of a binary archive containing:

- A signed container file containing the following elements:
  - The signed application binary file of the applet.
  - The public key matching the private key used to sign the application binary file of the applet.
  - The SafeSign IC PKI Applet v3 Interface Specification [FSP].
  - The test report of the applet.
  - An information file containing:
    - The used configuration.
    - The unique identifier of the toolchain versions.
    - The fingerprint of the used revision from all version control repositories.
    - The unique identifier of the applet.
- The preparative procedures document [PRE].
- The operational guidance document [OPE].

The customer is required to complete the TOE by installing the application binary file on the platform according to the guidance presented in the preparative procedures in order to meet the certified configuration of the TOE.

1.4 Compatibility Statement

The TSF for this TOE includes SFRs that rely on the TSF of the platform component. The compatibility of the platform TSF with the TOE TSF is confirmed by:

- The statement of the platform ST that it complies with the Java Card Protection Profile – Open Configuration, which defines the security mechanisms of the Java Card specification.

- Mapping the dependencies of specific TOE SFRs on identified security functionality provided by the platform in SF.Platform_Security_Functions (section 7.2.2),
- Following platform user guidance in development of the TOE and TOE guidance documentation.
- Ensuring the conformance claims made by the platform meet or supersedes the claims made by the TOE.

1.4.1 Platform SFRs Used By This Composite ST

The following table is a mapping of the SFRs listed in order of appearance in chapter 7 of [PST] and the SFRs of this ST.

Table 1. Mapping Platform SFR to usage by TOE SFR

Platform SFR	Used by TOE SFR	Remarks
COREG_LC Security Functional Requirements		
Firewall Policy		
FDP_ACC.2/FIREWALL	Not used	
FDP_ACF.1/FIREWALL	Not used	
FDP_IFC.1/JCVM	Not used	
FDP_IFF.1/JCVM	Not used	
FDP_RIP.1/OBJECTS	Not used	
FMT_MSA.1/JCRE	Not used	
FMT_MSA.1/JCVM	Not used	
FMT_MSA.2/FIREWALL_JCVM	Not used	
FMT_MSA.3/FIREWALL	Not used	
FMT_ MSA.3/JCVM	Not used	
FMT_ SMF.1	Not used	
FMT_ SMR.1	Not used	
Application Programming Interface		
FCS_CKM.1	FCS_CKM.1/ECC, FCS_CKM.1/RSA	
FCS_CKM.4	FCS_CKM.4	
FCS_COP.1	FCS_COP.1/ECC, FCS_COP.1/RSA	
FDP_RIP.1/ABORT	Not used	
FDP_RIP.1/APDU	Not used	
FDP_RIP.1/GlobalArray_Refined	Not used	
FDP_RIP.1/bArray	Not used	
FDP_RIP.1/KEYS	FDP_RIP.1	

FDP_RIP.1/TRANSIENT	Not used	
FDP_ROL.1/FIREWALL	Not used	
Card Security Management		
FAU_ARP.1	FPT_FLS.1, FPT_PHP.1	
FDP_SDI.2/DATA	FDP_SDI.2/Persistent, FDP_SDI.2/DTBS	
FDP_SDI.2/SENSITIVE_RESULT	Not used	
FPR_UNO.1	Not used	
FPT_FLS.1	FPT_FLS.1	
FPT_TDC.1	Not used	
Aid Management		
FIA_ATD.1/AID	Not used	
FIA_UID.2/AID	Not used	
FIA_USB.1/AID	Not used	
FMT_MTD.1/JCRE	Not used	
FMT_MTD.3/JCRE	Not used	
INSTG Security Functional Requirements		
FMT_SMR.1/Installer	Not used	
FPT_FLS.1/Installer	Not used	
FPT_RCV.3/Installer	Not used	
ADELG Security Functional Requirements		
FDP_ACC.2/ADEL	Not used	
FDP_ACF.1/ADEL	Not used	
FDP_RIP.1/ADEL	Not used	
FMT_MSA.1/ADEL	Not used	
FMT_MSA.3/ADEL	Not used	
FMT_SMF.1/ADEL	Not used	
FMT_SMR.1/ADEL	Not used	
FPT_FLS.1/ADEL	Not used	
RMIG Security Functional Requirements		
ODELG Security Functional Requirements		
FDP_RIP.1/ODEL	Not used	
FPT_FLS.1/ODEL	Not used	
CarG Security Functional Requirements		

FDP_UIT.1/CCM	Not used	
FDP_ROL.1/CCM	Not used	
FDP_ITC.2/CCM	Not used	
FPT_FLS.1/CCM	Not used	
FDP_ACC.1/SD	Not used	
FDP_ACF.1/SD	Not used	
FMT_MSA.1/SD	Not used	
FMT_MSA.3/SD	Not used	
FMT_SMF.1/SD	Not used	
FMT_SMR.1/SD	Not used	
FCO_NRO.2/SC	Not used	
FDP_IFC.2/SC	Not used	
FDP_IFF.1/SC	Not used	
FMT_MSA.1/SC	Not used	
FMT_MSA.3/SC	Not used	
FMT_SMF.1/SC	Not used	
FMT_UID.1/SC	Not used	
FIA_UAU.1/SC	Not used	
FIA_UAU.4/SC	Not used	
FTP_ITC.1/SC	FTP_ITC.1/SCD	
EMG Security Functional Requirements		
FDP_ACC.1/EXT_MEM	Not used	
FDP_ACF.1/EXT_MEM	Not used	
FMT_MSA.1/EXT_MEM	Not used	
FMT_MSA.3/EXT_MEM	Not used	
FMT_SMF.1/EXT_MEM	Not used	
ConfG Configuration Security Functionality		
FDP_IFC.2/CFG	Not used	
FDP_IFF.1/CFG	Not used	
FMT_MSA.1/CFG	Not used	
FMT_MSA.3/CFG	Not used	
FMT_SMF.1/CFG	Not used	
FMT_SMR.1/CFG	Not used	
FIA_UID.1/CFG	Not used	

SecBoxG SecureBox Security Functional Requirements		
FDP_ACC.2/SecureBox	Not used	
FDP_ACF.1/SecureBox	Not used	
FMT_MSA.1/SecureBox	Not used	
FMT_MSA.3/SecureBox	Not used	
FMT_SMF.1/SecureBox	Not used	
ModDesG Security Functional Requirements		
FDP_IFC.1/MODULAR_DESIGN	Not used	
FDP_IFF.1/MODULAR_DESIGN	Not used	
FIA_ATD.1/MODULAR_DESIGN	Not used	
FIA_UID.1/MODULAR_DESIGN	Not used	
FIA_USB.1/MODULAR_DESIGN	Not used	
FMT_MSA.1/MODULAR_DESIGN	Not used	
FMT_MSA.3/MODULAR_DESIGN	Not used	
FMT_SMF.1/MODULAR_DESIGN	Not used	
FMT_SMR.1/MODULAR_DESIGN	Not used	
FPT_FLS.1/MODULAR_DESIGN	Not used	
RMG Security Functional Requirements		
FDP_ACC.2/RM	Not used	
FDP_ACF.1/RM	Not used	
FMT_MSA.1/RM	Not used	
FMT_MSA.3/RM	Not used	
FMT_SMF.1/RM	Not used	
FIA_UID.1/RM	Not used	
FIA_UAU.1/RM	Not used	
Further Security Functional Requirements		
FAU_SAS.1/SCP	Not used	
FCS_RNG.1	FCS_CKM.1/ECC, FCS_CKM.1/RSA	
FCS_RNG.1/HDT	Not used	
FIA_AFL.1/PIN	FIA_AFL.1	
FPT_EMSEC.1	FPT_EMS.1	
FPT_PHP.3	FPT_PHP.1, FPT_PHP.3	
FCS_CKM.2	Not used	

FCS_CKM.3	Not used	

1.4.2 Security Assurance Requirements Mapping

The platform is certified EAL6 with augmentations ALC_FLR.1 and ASE_TSS.2. The TOE certification level is EAL4 augmented with AVA_VAN.5. The Composite TOE assurance requirements of the EAL4 package augmented with AVA_VAN.5 are a subset of the platform EAL6 package.

1.4.3 Compatibility Mapping Between This ST and the Platform ST

This section provides a listing of the platform ST security objectives, and security problem definitions, indicating for each item if this ST contradicts it, or how it is handled by this ST.

1.4.3.1 TOE Security Objectives

Table 2. Platform TOE security objectives mapping

Platform TOE security objectives	Contradiction/mapping	Remark
Identification		
OT.SID	None	
OT.SID_MODULE	None	
Execution		
OT.FIREWALL	None	
OT.GLOBAL_ARRAYS_CONFID	None	
OT.GLOBAL_ARRAYS_INTEG	Maps to OT.DTBS_Integrity_TOE	
OT.NATIVE	None	
OT.OPERATE	None	
OT.REALLOCATION	None	
OT.RESOURCES	None	
OT.SENSITIVE_RESULTS_INTEG	Maps to OT.Sigy_SigF	
Services		
OT.ALARM	Maps to OT.Tamper_ID, OT.Tamper_Resistance	
OT.CIPHER	None	
OT.RNG	Maps to OT.SCD_Unique	
OT.KEY-MNGT	Maps to OT.SCD_Secrecy, OT.Sigy_SigF, OT.SCD/SVD_Auth_Gen, OT.SCD_Unique, OT.SCD_SVD_Corresp, OT.SCD_Auth_Imp	
OT.PIN-MNGT	Maps to OT.Sigy_SigF, OT.SCD/SVD_Auth_Gen,	

	OT.SCD_Auth_Imp	
OT.TRANSACTION	None	
Object Deletion		
OT.OBJ-DELETION	None	
Applet Management		
OT.APPLI-AUTH	None	
OT.DOMAIN-RIGHTS	None	
OT.COMM_AUTH	None	
OT.COMM_INTEGRITY	None	
OT.COMM_CONFIDENTIALITY	None	
External Memory		
OT.EXT-MEM	None	
Card Management		
OT.CARD-MANAGEMENT	None	
Smart Card Platform		
OT.SCP.IC	Maps to OT.EMSEC_Design, OT.Tamper_ID, OT.Tamper_Resistance	
OT.SCP.RECOVERY	None	
OT.SCP.SUPPORT	None	
OT.IDENTIFICATION	None	
SecureBox		
OT.SEC_BOX_FW	None	
Random Numbers		
OT.RND	Maps to OT.SCD_Unique	
Configuration Module		
OT.CARD-CONFIGURATION	None	
Restricted Mode		
OT.ATTACK-COUNTER	Maps to OT.Tamper_Resistance	
OT.RESTRICTED-MODE	Maps to OT.Tamper_Resistance	

1.4.3.2 Environmental Objectives

Table 3. Platform environmental objectives mapping

Platform Environmental	Contradiction/mapping	Remark

Objectives		
OE.APPLET	Maps to [PRE]	
OE.VERIFICATION	Maps to [PRE]	
OE.CODE-EVIDENCE	Maps to [PRE]	
OE.APPS-PROVIDER	Maps to [PRE]	
OE.VERIFICATION-AUTHORITY	Maps to [PRE]	
OE.KEY-CHANGE	Maps to [PRE]	
OE.SECURITY-DOMAINS	Not contradicting.	
OE.USE_DIAG	Maps to [PRE], OE.SCD_Secrecy	
OE.USE_KEYS	Maps to OE.SVD_Auth, OE.SCD/SVD_Auth_Gen, OE.SCD_Secrecy, OE.SCD_Unique, OE.SCD_SVD_Corresp	
OE.PROCESS_SEC_IC	Mapped to [PRE]	

1.4.3.3 Threats

Table 4. Platform threats mapping

Platform Threats	Contradiction/mapping	Remark
Confidentiality		
T.CONFID-APPLI-DATA	Maps to T.SCD_Divulg, T.SCD_Derive, T.Hack_Phys, T.SigF_Misuse	
T.CONFID-JCS-CODE	None	
T.CONFID-JCS-DATA	None	
Integrity		
T.INTEG-APPLI-CODE	None	
T.INTEG-APPLI-CODE.LOAD	None	
T.INTEG-APPLI-DATA[REFINED]	Maps to T.SCD_Divulg, T.SCD_Derive, T.Hack_Phys, T.SigF_Misuse	
T.INTEG-APPLI-DATA.LOAD	None	
T.INTEG-JCS-CODE	None	
T.INTEG-JCS.DATA	None	
Identity Usurpation		
T.SID.1	None	

T.SID.2	Maps to T.SCD_Divulg, T.Hack_Phys, T.SigF_Misuse	
Unauthorized Execution		
T.EXE-CODE.1	None	
T.EXE-CODE.2	None	
T.NATIVE	None	
T.MODULE_EXEC	None	
Denial of Service		
T.RESOURCES	None	
Card Management		
T.UNAUTHORIZED_CARD_MNGT	None	
T.COM_EXPLOIT	None	
T.LIFE_CYCLE	None	
Services		
T.OBJ-DELETION	None	
Miscellaneous		
T.PHYSICAL	Maps to T.Hack_Phys	
Operating System		
T.OS_OPERATE	None	
Random Numbers		
T.RND	Maps to T.SCD_Derive	
Configuration Module		
T.CONFIG	None	
Secure Box		
T.SEC_BOX_BORDER	None	
Module Replacement		
T.MODULE_REPLACEMENT	None	
Restricted Mode		
T.ATTACK_COUNTER	None	

1.4.3.4 Assumptions

Table 5. Platform assumptions mapping

Platform Assumptions	Contradiction/mapping	Remark
A.APPLET	Maps to [PRE]	
A.VERIFICATION	Maps to [PRE]	

A.USE_DIAG	Maps to A.SCA, OE.HID_VAD, OE.DTBS_Protect	
A.USE_KEYS	Maps to A.CGA, A.SCA, A.CSP	
A.PROCESS-SEC-IC	Maps to [PRE]	
A.APPS-PROVIDER	Maps to [PRE]	
A.VERIFICATION-AUTHORITY	Maps to [PRE]	

1.4.3.5 Organizational Security Policies

Table 6. Platform organizational security policies mapping

Platform OSPs	Contradiction/mapping	Remark
OSP.VERIFICATION	Maps to [PRE]	
OSP.PROCESS-TOE	Maps to [PRE], [OPE]	
OSP.KEY-CHANGE	Maps to [PRE]	
OSP.SECURITY-DOMAINS	Not contradicting	
OSP.SECURE-BOX	Not contradicting	

2 Conformance Claims

2.1 CC Conformance Claim

This Security Target claims to be conformant to the Common Criteria for Information Technology Security Evaluation version 3.1 according to:

- “Common Criteria for Information Technology Security Evaluation, Part 1, Version 3.1, Revision 5, April 2017” [CC1]
- “Common Criteria for Information Technology Security Evaluation, Part 2, Version 3.1, Revision 5, April 2017” [CC2]
- “Common Criteria for Information Technology Security Evaluation, Part 3, Version 3.1, Revision 5, April 2017” [CC3]

This Security Target claims to be CC Part 2 extended and CC Part 3 conformant.

The methodology “Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5” [CEM] will be used for the evaluation.

2.2 PP Conformance Claim

This Security Target claims strict conformance with EN-419211-2:2013 Protection profiles for secure signature creation device - Part 2: Device with key generation (v2.0.1, BSI-CC-PP-0059-2009-MA-02) [PP2] and with EN-419211-3:2013 Protection profiles for secure signature creation device - Part 3: Device with key import (v1.0.2, BSI-CC-PP-0075-2012-MA-01) [PP3].

2.3 Package Claim

This Security Target claims conformance with assurance package EAL4 augmented with AVA_VAN.5 (“Advanced methodical vulnerability analysis”).

2.4 Conformance Rationale

This ST conforms to all elements in both PPs. Where there is no full overlap between the PPs, the combination of the two is taken. This is marked throughout this document.

3 Security Problem Definition

3.1 Users

The following users are taken directly from the PPs and are also present in this TOE.

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

3.2 Assets

The following assets are taken directly from the PPs and are also present in this TOE.

- SCD Private key used to perform an electronic signature operation.
  The confidentiality, integrity and signatory's sole control over the use of the SCD shall be maintained.
- SVD Public key linked to the SCD and used to perform electronic signature verification.
  The integrity of the SVD when it is exported shall be maintained.
- DTBS and DTBS/R 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 shall be maintained.

3.3 Threats

The attacker model is taken from the PPs;

- 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.

The following threats are taken from the PPs:

- 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 that 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.

3.4 Organizational Security Policies (OSPs)

Organizational Security Policies are taken from the PP:

- P.CSP_QCert Qualified certificate.
  The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate for the SVD. 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, which is a qualified electronic signature if it is based on a valid qualified certificate. 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.
- P.Sigy_SSCD TOE as secure signature creation device.
  The TOE meets the requirements for an SSCD laid down in Annex III of DIRECTIVE 1999/93/EC. 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.

3.5 Assumptions

The following assumptions are taken from the PPs:

- 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 the data the signatory wishes to sign in a form appropriate for signing by the TOE.

The following assumption is only taken from the EN-419211-3 PP [PP3] and has no impact on the EN-419211-2 PP [PP2] (as in this PP the TOE is responsible and no assumption is needed).

- 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.

4 Security Objectives

4.1 Security Objectives for the TOE

The following security objectives for the TOE are taken from the PPs:

- OT.Lifecycle_Security Lifecycle security.
  The TOE shall detect flaws during the initialisation, personalisation and operational usage. The TOE shall securely destroy the SCD on demand of the signatory.
- 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.
- 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.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.DTBS_Integrity_TOE DTBS/R integrity inside the TOE.
  The TOE shall 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.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.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.Tamper_Resistance Tamper resistance.
  The TOE shall prevent or resist physical tampering with specified system devices and components.

The following security objectives for the TOE are taken from the EN-419211-2 PP [PP2]:

- OT.SCD/SVD_Auth_Gen Authorised 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.
- 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_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.

The following security objective for the TOE is taken from the EN-419211-3 PP [PP3]:

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

4.2 Security Objectives for the Operational Environment

The following security objectives for the Operational Environment are taken from the PPs:

- 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):
  a) the name of the signatory controlling the TOE;
  b) the SVD matching the SCD stored in the TOE and being under sole control of the signatory;
  c) 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.
- OE.SSCD_Prov_Service Authentic SSCD provided by SSCD-provisioning service.
  The SSCD-provisioning service shall initialise and personalise for the signatory an authentic copy of the TOE and deliver this copy as SSCD to the signatory.
- OE.HID_VAD Protection of the VAD.
  If an external device provides the human interface for user authentication, this device shall 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. In

particular, if the TOE requires a trusted channel for import of the VAD, the HID shall support usage of this trusted channel.

- OE.DTBS_Intend SCA sends data intended to be signed.
  The signatory shall use a trustworthy SCA that:
  - 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;
  - sends the DTBS/R to the TOE and enables verification of the integrity of the DTBS/R by the TOE;
  - attaches the signature produced by the TOE to the data or provides it separately.
- OE.DTBS_Protect SCA protects the data intended to be signed.
  The operational environment shall ensure that the DTBS/R cannot be altered in transit between the SCA and the TOE. In particular, if the TOE requires a trusted channel for import of the DTBS/R, the SCA shall support usage of this trusted channel.
- 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.

The following security objectives for the Operational Environment are taken from the EN-419211-3 PP [PP3] and only apply in case of key import:

- OE.SCD/SVD_Auth_Gen Authorised 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.
- 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_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_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 send to the CGA and the SCD exported to the TOE of the signatory identified in the SVD certificate.

4.3 Security Objectives Rationale

The security objectives rationale is outlined by the PPs. The specifics will not be repeated here, but the combined tracing tables are given below.

Table 7. Security objectives for the TOE tracing

	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Auth_Imp
T.SCD_Divulg		X										X
T.SCD_Derive			X						X			
T.Hack_Phys		X				X	X	X				
T.SVD_Forgery											X	
T.SigF_Misuse	X			X	X							
T.DTBS_Forgery					X							
T.Sig_Forgery			X							X		
P.CSP_QCert	X										X	X
P.QSign			X	X								
P.Sigy_SSCD	X	X	X	X	X	X		X	X	X		X
P.Sig_Non-Repud	X	X	X	X	X	X	X	X		X	X	
A.CGA												
A.SCA												
A.CSP												

Table 8. Security objectives for the operational environment tracing

	OE.SVD_Auth	OE.CGA_QCert	OE.SSCD_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory	OE.SCD/SVD_Auth_Gen	OE.SCD_Secrecy	OE.SCD_Unique	OE.SCD_SVD_Corresp
T.SCD_Divulg								X	X		
T.SCD_Derive										X	
T.Hack_Phys											
T.SVD_Forgery	X										X
T.SigF_Misuse				X	X	X	X				

T.DTBS_Forgery					X	X					
T.Sig_Forgery		X								X	
P.CSP_QCert		X						X			X
P.QSign		X			X						
P.Sigy_SSCD			X					X	X	X	
P.Sig_Non-Repud	X	X	X		X	X	X		X	X	X
A.CGA	X	X									
A.SCA					X						
A.CSP								X	X	X	X

5 Extended Components Definition

The additional family FPT_EMS (TOE Emanation) of the Class FPT (Protection of the TSF) is defined here to describe the IT security functional requirements of the TOE. The TOE shall prevent attacks against the SCD and other secret data where the attack is based on external observable physical phenomena of the TOE. Examples of such attacks are evaluation of TOE's electromagnetic radiation, simple power analysis (SPA), differential power analysis (DPA), timing attacks, radio emanation, etc. This family describes the functional requirements for the limitation of intelligible emanations. The family FPT_EMS belongs to the Class FPT because it is the class for TSF protection. Other families within the Class FPT do not cover the TOE emanation. The definition of the family FPT_EMS is taken from the EN-419211-2 and EN-419211-3 PPs [PP2, PP3].

5.1 FPT_EMS TOE Emanation

Family behaviour:

This family defines requirements to mitigate intelligible emanations.

Component levelling:

FPT_EMS TOE Emanation	1

FPT_EMS.1 TOE Emanation has two constituents:

- **FPT_EMS.1.1** Limit of Emissions requires to not emit intelligible emissions enabling access to TSF data or user data.
- **FPT_EMS.1.2** Interface Emanation requires to not emit interface emanation enabling access to TSF data or user data.

Management: FPT_EMS.1

There are no management activities foreseen.

Audit: FPT_EMS.1

There are no actions identified that shall be auditable if FAU_GEN (Security audit data generation) is included in a PP or ST using FPT_EMS.1.

5.1.1 FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

- FPT_EMS.1.1 The TOE shall not emit [assignment: types of emissions] in excess of [assignment: specified limits] enabling access to [assignment: list of types of TSF data] and [assignment: list of types of user data].
- FPT_EMS.1.2 The TSF shall ensure [assignment: type of users] are unable to use the following interface [assignment: type of connection] to gain access to [assignment: list of types of TSF data] and [assignment: list of types of user data].

6 Security Requirements

6.1 Security Functional Requirements

6.1.1 Cryptographic support (FCS)

6.1.1.1 FCS_CKM.1/ECC Cryptographic key generation

Hierarchical to: No other components.

Dependencies:
[FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1
The TSF shall generate an SCD/SVD pair in accordance with a specified cryptographic key generation algorithm JCOP RNG and specified cryptographic key sizes ECC 256, 384, 512, 521 bit that meet the following: BSI TR-02102-1 v2020-01.

- [assignment: cryptographic key generation algorithm] → JCOP RNG; According to JCOP 4 P71 [PST].
- [assignment: cryptographic key sizes] → ECC 256, 384, 512, 521 bit; According to JCOP 4 P71 [PST] and BSI TR-02102-1 [BSI].
- [assignment: list of standards] → BSI TR-02102-1 v2020-01; ref [BSI].

6.1.1.2 FCS_CKM.1/RSA Cryptographic key generation

Hierarchical to: No other components.

Dependencies:
[FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1
The TSF shall generate an SCD/SVD pair in accordance with a specified cryptographic key generation algorithm JCOP RNG and specified cryptographic key sizes RSA from 2000 to 4096 bit that meet the following: BSI TR-02102-1 v2020-01.

- [assignment: cryptographic key generation algorithm] → JCOP RNG; According to JCOP 4 P71 [PST].

- [assignment: cryptographic key sizes] → RSA from 2000 to 4096 bit; According to JCOP 4 P71 [PST] and BSI TR-02102-1 [BSI].
- [assignment: list of standards] → BSI TR-02102-1 v2020-01; ref [BSI].

6.1.1.3 FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

Dependencies:
[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1
The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **physically overwriting the keys in a randomized manner** that meets the following: **none**.

- [assignment: cryptographic key destruction method] → physically overwriting the keys in a randomized manner; According to JCOP 4 P71 [PST].
- [assignment: list of standards] → none; According to JCOP 4 P71 [PST].

6.1.1.4 FCS_COP.1/ECC Cryptographic operation

Hierarchical to: No other components.

Dependencies:
[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1
The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm **ECDSA** and cryptographic key sizes **ECC 256, 384, 512, 521 bit** that meet the following: **Regulation (EU) No 910/2014**.

- [assignment: cryptographic algorithm] → ECDSA; According to JCOP 4 P71 [PST].
- [assignment: cryptographic key sizes] → ECC 256, 384, 512, 521 bit; According to JCOP 4 P71 [PST] and BSI TR-02102-1 [BSI].
- [assignment: list of standards] → Regulation (EU) No 910/2014; ref [EU].

6.1.1.5 FCS_COP.1/RSA Cryptographic operation

Hierarchical to: No other components.

Dependencies:
[FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1
The TSF shall perform digital signature creation in accordance with a specified cryptographic algorithm **RSA signature with PKCS#1 padding** and cryptographic key sizes **RSA from 2000 to 4096 bit** that meet the following: **Regulation (EU) No 910/2014**.

- [assignment: cryptographic algorithm] → RSA signature with PKCS#1 padding; According to JCOP 4 P71 [PST].
- [assignment: cryptographic key sizes] → RSA from 2000 to 4096 bit; According to JCOP 4 P71 [PST] and BSI TR-02102-1 [BSI].
- [assignment: list of standards] → Regulation (EU) No 910/2014; ref [EU].

6.1.2 User data protection (FDP)

6.1.2.1 FDP_ACC.1/SCD/SVD_Generation Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/SCD/SVD_Generation
The TSF shall enforce the SCD/SVD Generation SFP on:
1) subjects: S.User,
2) objects: SCD, SVD,
3) operations: generation of SCD/SVD pair.

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

Hierarchical to: No other components.

Dependencies:
FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

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.

6.1.2.3 FDP_ACC.1/SVD_Transfer Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/SVD_Transfer
The TSF shall enforce the SVD Transfer SFP on:
1) subjects: S.User;
2) objects: SVD;
3) operations: export.

6.1.2.4 FDP_ACF.1/SVD_Transfer Security attribute based access control

Hierarchical to: No other components.

Dependencies:
FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1/SVD_Transfer
The TSF shall enforce the SVD Transfer SFP to objects based on the following:
1) the S.User is associated with the security attribute Role;
2) 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 are allowed to export SVD.

- [selection: R.Admin, R.Sigy] → R.Admin and R.Sigy are.

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.

6.1.2.5 FDP_ACC.1/SCD_Import Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/SCD_Import
The TSF shall enforce the SCD Import SFP on
(1) subjects: S.User,
(2) objects: SCD,
(3) operations: import of SCD.

6.1.2.6 FDP_ACF.1/SCD_Import Security attribute based access control

Hierarchical to: No other components.

Dependencies:
FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/SCD_Import
The TSF shall enforce the SCD Import SFP to objects based on the following: the 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.

6.1.2.7 FDP_ACC.1/Signature_Creation Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1/Signature_Creation
The TSF shall enforce the Signature Creation SFP on:
1) subjects: S.User;
2) objects: DTBS/R, SCD;
3) operations: signature creation.

6.1.2.8 FDP_ACF.1/Signature_Creation Security attribute based access control

Hierarchical to: No other components.

Dependencies:
FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1/Signature_Creation
The TSF shall enforce the Signature Creation SFP to objects based on the following:
1) the user S.User is associated with the security attribute “Role”; and
2) 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”.

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

Hierarchical to: No other components.

Dependencies:
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.3 Static attribute initialisation

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
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: none.

- [assignment: additional importation control rules] → none.

6.1.2.10 FDP_UCT.1/SCD Basic data exchange confidentiality

Hierarchical to: No other components.

Dependencies:
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

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

6.1.2.11 FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

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

6.1.2.12 FDP_SDI.2/Persistent Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies.

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:
1) prohibit the use of the altered data;
2) inform the S.Sigy about integrity error.

6.1.2.13 FDP_SDI.2/DTBS Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring.

Dependencies: No dependencies.

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:

1) prohibit the use of the altered data;
2) inform the S.Sigy about integrity error.

6.1.3 Identification and authentication (FIA)

6.1.3.1 FIA_UID.1 Timing of identification

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_UID.1.1
The TSF shall allow:
1) self-test according to FPT_TST.1;
2) none
on behalf of the user to be performed before the user is identified.

- [assignment: list of additional TSF-mediated actions] → none.

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.

6.1.3.2 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FIA_UAU.1.1
The TSF shall allow:
1) self-test according to FPT_TST.1;
2) identification of the user by means of TSF required by FIA_UID.1;
3) none
on behalf of the user to be performed before the user is authenticated.

- [assignment: list of additional TSF-mediated actions] → none.

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.

6.1.3.3 FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1
The TSF shall detect when an administrator configurable positive integer within the range from 1 to 15 unsuccessful authentication attempts occur related to consecutive failed authentication attempts.

- [selection: [assignment: positive integer number], an administrator configurable positive integer within [assignment: range of acceptable values]] → an administrator configurable positive integer within [assignment: range of acceptable values].
- [assignment: range of acceptable values] → the range from 1 to 15.

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

6.1.4 Security management (FMT)

6.1.4.1 FMT_SMR.1 Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification.

FMT_SMR.1.1
The TSF shall maintain the roles R.Admin and R.Sigy.

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

6.1.4.2 FMT_SMF.1 Security management functions

Hierarchical to: No other components.

Dependencies: No dependencies.

FMT_SMF.1.1
The TSF shall be capable of performing the following management functions:
1) creation and modification of 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.

- [assignment: list of other security management functions to be provided by the TSF] → none.

6.1.4.3 FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies:
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions.

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

6.1.4.4 FMT_MSA.1/Admin Management of security attributes

Hierarchical to: No other components.

Dependencies:
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1/Admin
The TSF shall enforce the SCD/SVD Generation SFP and SCD Import SFP to restrict the ability to modify, none, the security attributes SCD/SVD management to R.Admin.

- [assignment: other operations] → none.

Note that the security functional requirements FMT_MSA.1.1/Admin from the EN 419211-2 PP [PP2] and EN 419211-3 PP [PP3] are merged to include both SCD/SVD Generation and SCD Import.

6.1.4.5 FMT_MSA.1/Signatory Management of security attributes

Hierarchical to: No other components.

Dependencies:
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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

6.1.4.6 FMT_MSA.2 Secure security attributes

Hierarchical to: No other components.

Dependencies:
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.2.1

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

6.1.4.7 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies:
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

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.

Note that the security functional requirements FMT_MSA.3.1 from the EN 419211-2 PP [PP2] and EN 419211-3 PP [PP3] are merged to include both SCD/SVD Generation and SCD Import.

6.1.4.8 FMT_MSA.4 Security attribute value inheritance

Hierarchical to: No other components.

Dependencies:
[FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

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.

Note that the security functional requirements FMT_MSA.4.1 from the EN 419211-2 PP [PP2] and EN 419211-3 PP [PP3] are merged to include both SCD/SVD Generation and SCD Import.

6.1.4.9 FMT_MTD.1/Admin Management of TSF data

Hierarchical to: No other components.

Dependencies:
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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

6.1.4.10 FMT_MTD.1/Signatory Management of TSF data

Hierarchical to: No other components.

Dependencies:
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

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

- [assignment: other operations] → unblock; According to PPs EN 419211-2 [PP2] and EN 419211-3 [PP3].

6.1.5 Protection of the TSF (FPT)

6.1.5.1 FPT_EMS.1 TOE Emanation

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_EMS.1.1
The TOE shall not emit **variations in power consumption or timing during command execution** in excess of **non-useful information** enabling access to RAD and SCD.

- [assignment: types of emissions] → variations in power consumption or timing during command execution; According to JCOP 4 P71 [PST].
- [assignment: specified limits] → non-useful information; According to JCOP 4 P71 [PST].

FPT_EMS.1.2
The TSF shall ensure **that unauthorized users** are unable to use the following interface **electrical contacts or Radio Frequency (RF) field** to gain access to RAD and SCD.

- [assignment: type of users] → that unauthorized users.
- [assignment: type of connection] → electrical contacts or Radio Frequency (RF) field; According to JCOP 4 P71 [PST], this includes sending APDUs.

6.1.5.2 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

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) **control flow and authentication checks (in accordance with FPT_PHP), executed before cryptographic operations, fail**.

- [assignment: list of other types of failures in the TSF] → control flow and authentication checks (in accordance with FPT_PHP), executed before cryptographic operations, fail.

6.1.5.3 FPT_PHP.1 Passive detection of physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

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.

6.1.5.4 FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

Dependencies: No dependencies.

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.

- [assignment: physical tampering scenarios] → physical manipulation and physical probing; According to JCOP 4 P71 [PST].
- [assignment: list of TSF devices/elements] → TSF; According to JCOP 4 P71 [PST].

6.1.5.5 FPT_TST.1 TSF testing

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_TST.1.1
The TSF shall run a suite of self tests **at the conditions:**
1) during initial start-up
2) periodically during normal operation
to demonstrate the correct operation of the TSF.

- [selection: during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self-test should occur]] → at the conditions [assignment: conditions under which self-test should occur].
- [assignment: conditions under which self-test should occur] → during initial start-up, periodically during normal operation.

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

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

6.1.6 Trusted path/channels (FTP)

6.1.6.1 FTP_ITC.1/SCD Inter-TSF trusted channel

Hierarchical to: No other components.

Dependencies: No dependencies.

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
1) Data exchange integrity according to FDP_UCT.1/SCD,
2) none.

- [assignment: list of other functions for which a trusted channel is required] → none.

6.2 Security Assurance Requirements

Security assurance level EAL4 augmented with AVA_VAN.5.

Table 9. Security assurance overview

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description ADV_FSP.4 Complete functional specification ADV_IMP.1 Implementation representation of the TSF ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMS.4 Problem tracking CM coverage ALC_DEL.1 Delivery procedures

	ALC_DVS.1 Identification of security measures ALC_LCD.1 Developer defined life-cycle model ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage ATE_DPT.1 Testing: basic design ATE_FUN.1 Functional testing ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.5 Advanced methodical vulnerability analysis

6.3 Security Requirements Rationale

Coverage:

Table 10. SFRs to security objectives for the TOE tracing

	OT.Lifecycle_Security	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.SCD/SVD_Auth_Gen	OT.SCD_Unique	OT.SCD_SVD_Corresp	OT.SCD_Auth_Imp
FCS_CKM.1/ECC	X	X								X	X	
FCS_CKM.1/RSA	X	X								X	X	
FCS_CKM.4	X	X										
FCS_COP.1/ECC	X		X									
FCS_COP.1/RSA	X		X									
FDP_ACC.1/SCD/SVD_Generation	X								X			
FDP_ACC.1/SVD_Transfer	X											

FDP_ACC.1/SCD_Import	X											X
FDP_ACC.1/Signature_Creation	X			X								
FDP_ACF.1/SCD/SVD_Generation	X								X			
FDP_ACF.1/SVD_Transfer	X											
FDP_ACF.1/SCD_Import	X											X
FDP_ACF.1/Signature_Creation	X			X								
FDP_ITC.1/SCD	X											
FDP_RIP.1		X		X								
FDP_SDI.2/Persistent		X	X								X	
FDP_SDI.2/DTBS				X	X							
FDP_UCT.1/SCD	X	X										
FIA_AFL.1				X								
FIA_UAU.1				X					X			X
FIA_UID.1				X					X			X
FMT_MOF.1	X			X								
FMT_MSA.1/Admin	X								X			
FMT_MSA.1/Signatory	X			X								
FMT_MSA.2	X			X					X			
FMT_MSA.3	X			X					X			
FMT_MSA.4	X			X					X		X	
FMT_MTD.1/Admin	X			X								
FMT_MTD.1/Signatory	X			X								
FMT_SMR.1	X			X								
FMT_SMF.1	X			X							X	
FPT_EMS.1		X				X						
FPT_FLS.1		X										
FPT_PHP.1							X					
FPT_PHP.3		X						X				
FPT_TST.1	X	X	X									
FTP_ITC.1/SCD	X	X										

Sufficiency and satisfaction of dependencies of security requirements follow from the PPs will not be repeated here.

7 TOE Summary Specifications

7.1 Security Services

7.1.1 SS.Access_Control

The applet provides configurable access controls to manage the use of data object and cryptographic support.

Access control is configured by specifying the authentication objects, or combinations thereof, that are permitted access to perform read/write/use operations on objects.

This service provides:

- FDP_ACC.1/SCD/SVD_Generation: Access control lists are checked by the TOE before SCD/SVD generation.
- FDP_ACC.1/SVD_Transfer: Access control lists are checked by the TOE before SVD transfer.
- FDP_ACC.1/SCD_Import: Access control lists are checked by the TOE before SCD import.
- FDP_ACC.1/Signature_Creation: Access control lists are checked by the TOE before signature creation.
- FDP_ACF.1/SCD/SVD_Generation: Access control lists are checked by the TOE before SCD/SVD generation.
- FDP_ACF.1/SVD_Transfer: Access control lists are checked by the TOE before SVD transfer.
- FDP_ACF.1/SCD_Import: Access control lists are checked by the TOE before SCD import.
- FDP_ACF.1/Signature_Creation: Access control lists are checked by the TOE before signature creation.
- FDP_ITC.1/SCD: Access control lists are checked by the TOE before SCD import.
- FIA_UAU.1: Access control lists prevent other TSF-mediated actions before authentication.
- FIA_UID.1: Access control lists prevent other TSF-mediated actions before identification.
- FMT_MOF.1: Access control lists are checked by the TOE before TOE activation by the signatory.
- FMT_MSA.1/Admin: Access control lists are checked by the TOE before security attribute modification.
- FMT_MSA.1/Signatory: Access control lists are checked by the TOE before security attribute modification.
- FMT_MSA.3: Access control lists are checked by the TOE before security attribute initialization.
- FMT_MSA.4: Access control lists are checked by the TOE before SCD/SVD generation SCD and import.
- FMT_MTD.1/Admin: Access control lists are checked by the TOE before RAD creation.
- FMT_MTD.1/Signatory: Access control lists are checked by the TOE before RAD modification.

7.1.2 SS.Authentication_Management

Security management allows blocking, unblocking and modification of authentication objects. These operations are subject to access control.

This service provides:

- FIA_AFL.1: The TOE allows the configurable number of unsuccessful authentication attempts upon construction of the authentication object. This cannot be modified afterwards.
- FMT_MSA.1/Admin: The security attribute “SCD/SVD Management” can only be set by the administrator upon construction of the authentication object. This cannot be modified afterwards.
- FMT_MSA.2: Only secure values are accepted for security attribute “SCD/SVD Management”.
- FMT_MTD.1/Admin: Creation functionality of a new RAD is provided by the TOE.
- FMT_MTD.1/Signatory: Modification functionality of a RAD is provided by the TOE.
- FMT_SMR.1: Users are associated with roles through authentication objects.
- FMT_SMF.1: Management functions of security attributes related to authentication objects are implemented by the TOE.

7.1.3 SS.Key_Management

Key Management provides the ability of import, export and destruction of keys. The ability is controlled by access control policies and properties defined by the object.

This service provides:

- FCS_CKM.4: Cryptographic key destruction is instrumented by the applet.
- FDP_ITC.1/SCD: Security attributes associated with the SCD are ignored as part of the SCD import process.
- FDP_RIP.1: References to keys are completely removed during key destruction.
- FDP_UCT.1/SCD: Imported SCDs are protected from unauthorized disclosure by symmetric key encryption.
- FMT_MSA.1/Signatory: The security attribute “SCD operational” can only be changed to yes by the signatory.
- FMT_MSA.2: Only secure values are accepted for security attribute “SCD operational”.
- FMT_MSA.3: Security attributes have to always be specified by the administrator.
- FMT_MSA.4: The security attribute “SCD operational” is set appropriately as part of the key import process.
- FMT_SMF.1: Management functions of security attributes related to keys are implemented by the TOE.

7.1.4 SS.RSA/ECC_Key_Generation

The TOE supports generation of cryptographic keys for usage. For this it uses the cryptographic libraries provided by the platform. Key generation is subject to access control.

This service provides:

- FCS_CKM.1/ECC: ECC key generation is instrumented by the applet.
- FCS_CKM.1/RSA: RSA key generation is instrumented by the applet.
- FMT_MSA.4: The security attribute “SCD operational” is set appropriately as part of the key generation process.

7.1.5 SS.RSA/ECC_Signature_Creation

The TOE supports the creation of signatures. For this it uses the cryptographic libraries provided by the platform. Signature creation is subject to access control.

This service provides:

- FCS_COP.1/ECC: ECC operations are instrumented by the applet to allow for signature creation.
- FCS_COP.1/RSA: RSA operations are instrumented by the applet to allow for signature creation.

7.1.6 SS.Secure_Messaging

The TOE utilizes the platform secure messaging services to provide authenticated and confidential communications with the TOE and external entities.

This service provides:

- FDP_UCT.1/SCD: The SCD is protected from unauthorized disclosure by the secure messaging channel.
- FTP_ITC.1/SCD: The secure messaging channel provides a logically distinct, authenticated channel with protection from modification and disclosure.

7.1.7 SS.User_Authentication

The TOE provides configurable authentication mechanisms to be used by SS.Access_Control for operating the TOE security functionality.

This service provides:

- FDP_ACC.1/SCD/SVD_Generation: The user needs to be authenticated to the TOE as input for SS.Access_Control.
- FDP_ACC.1/SVD_Transfer: The user needs to be authenticated to the TOE as input for SS.Access_Control.
- FDP_ACC.1/SCD_Import: The user needs to be authenticated to the TOE as input for SS.Access_Control.
- FDP_ACC.1/Signature_Creation: The user needs to be authenticated to the TOE as input for SS.Access_Control.
- FDP_ACF.1/SCD/SVD_Generation: The user needs to be authenticated to the TOE as input for SS.Access_Control.
- FDP_ACF.1/SVD_Transfer: The user needs to be authenticated to the TOE as input for SS.Access_Control.
- FDP_ACF.1/SCD_Import: The user needs to be authenticated to the TOE as input for SS.Access_Control.
- FDP_ACF.1/Signature_Creation: The user needs to be authenticated to the TOE as input for SS.Access_Control.
- FIA_AFL.1: Authentication failure is handled by returning an error code containing also the number of tries remaining. After an authentication failure, the corresponding authentication object is guaranteed to not be authenticated.
- FIA_UAU.1: The user is authenticated after a successful authentication.
- FIA_UID.1: The user is identified as part of the authentication process.

7.2 Security Features

7.2.1 SF.Applet_Hardening

Specific coding strategies are applied to strengthen the applet resilience against advanced attack types such as fault injection and side channel analysis.

This feature, combined with the underlying platform security features, realizes:

- FPT_EMS.1: The TOE relies on the platform where possible for critical code execution. When not possible, for critical code, coding strategies that minimize emanation are used.
- FPT_FLS.1: The TOE does not modify state before all tests have been checked.
- FPT_PHP.1: The TOE uses control flow monitoring and defensive coding strategies.
- FPT_PHP.3: The TOE requires additional security checks to pass before executing critical sections.
- FPT_TST.1: The self test of the TOE is ran during applet selection, and randomly while processing APDU commands.

7.2.2 SF.Platform_Security_Functions

The TOE is a composite product and uses security services and security features provided by the underlying platform. See the JCOP 4 P71 Security Target Lite [PST] for an overview of security features provided by the platform. This security feature defines the combined platform security services and security features used for realizing the security functional requirements in this TOE.

This feature realizes:

- FCS_CKM.1/ECC: The TOE uses the platform cryptographic libraries for its ECC key generation (SF.CRYPTO: Cryptographic Functionality).
- FCS_CKM.1/RSA: The TOE uses the platform cryptographic libraries for its RSA key generation (SF.CRYPTO: Cryptographic Functionality).
- FCS_CKM.4: The TOE uses the platform cryptographic libraries for its cryptographic key destruction (SF.CRYPTO: Cryptographic Functionality).
- FCS_COP.1/ECC: The TOE uses the platform cryptographic libraries for its ECC operations (SF.CRYPTO: Cryptographic Functionality).
- FCS_COP.1/RSA: The TOE uses the platform cryptographic libraries for its RSA operations (SF.CRYPTO: Cryptographic Functionality).
- FDP_SDI.2/Persistent: The TOE uses the platform for integrity checks (SF.JCVM: Java Card Virtual Machine).
- FDP_SDI.2/DTBS: The TOE uses the platform for integrity checks (SF.JCVM: Java Card Virtual Machine).
- FIA_AFL.1: The TOE uses the platform to keep track of failed authentication attempts and blocking the RAD after this has met the configurable number of attempts (SF.PIN: PIN Management).
- FPT_EMS.1: The TOE uses the platform's emanation protection (SF.SMG_NSC: No Side-Channel).
- FPT_FLS.1: Realized by the platform tearing, transaction, and memory management functions (SF.PERS_MEM: Persistent Memory Management).

- **FPT_PHP.1**: The TOE uses the platform's physical attack detection (SF.HW_EXC: Hardware Exception Handling).
- **FPT_PHP.3**: The TOE uses the platform's physical attack resistance (SF.HW_EXC: Hardware Exception Handling).
- **FTP_ITC.1/SCD**: The TOE uses the platform's secure channel implementation (SF.OPEN: Card Content Management).

7.3 TOE Summary Specification Rationale

Table 11. SFRs to security services/features tracing

	SS.Access_Control	SS.Authentication_Management	SS.Key_Management	SS.RSA/ECC_Key_Generation	SS.RSA/ECC_Signature_Creation	SS.Secure_Messaging	SS.User_Authentication	SF.Applet_Hardening	SF.Platform_Security_Functions
FCS_CKM.1/ECC				X					X
FCS_CKM.1/RSA				X					X
FCS_CKM.4			X						X
FCS_COP.1/ECC					X				X
FCS_COP.1/RSA					X				X
FDP_ACC.1/SCD/SVD_Generation	X						X		
FDP_ACC.1/SVD_Transfer	X						X		
FDP_ACC.1/SCD_Import	X						X		
FDP_ACC.1/Signature_Creation	X						X		
FDP_ACF.1/SCD/SVD_Generation	X						X		
FDP_ACF.1/SVD_Transfer	X						X		
FDP_ACF.1/SCD_Import	X						X		
FDP_ACF.1/Signature_Creation	X						X		
FDP_ITC.1/SCD	X		X						
FDP_RIP.1			X						
FDP_SDI.2/Persistent									X
FDP_SDI.2/DTBS									X
FDP_UCT.1/SCD			X			X			

FIA_AFL.1		X					X		X
FIA_UAU.1	X						X		
FIA_UID.1	X						X		
FMT_MOF.1	X								
FMT_MSA.1/Admin	X	X							
FMT_MSA.1/Signatory	X		X						
FMT_MSA.2		X	X						
FMT_MSA.3	X		X						
FMT_MSA.4	X		X	X					
FMT_MTD.1/Admin	X	X							
FMT_MTD.1/Signatory	X	X							
FMT_SMR.1		X							
FMT_SMF.1		X	X						
FPT_EMS.1								X	X
FPT_FLS.1								X	X
FPT_PHP.1								X	X
FPT_PHP.3								X	X
FPT_TST.1								X	
FTP_ITC.1/SCD						X			X