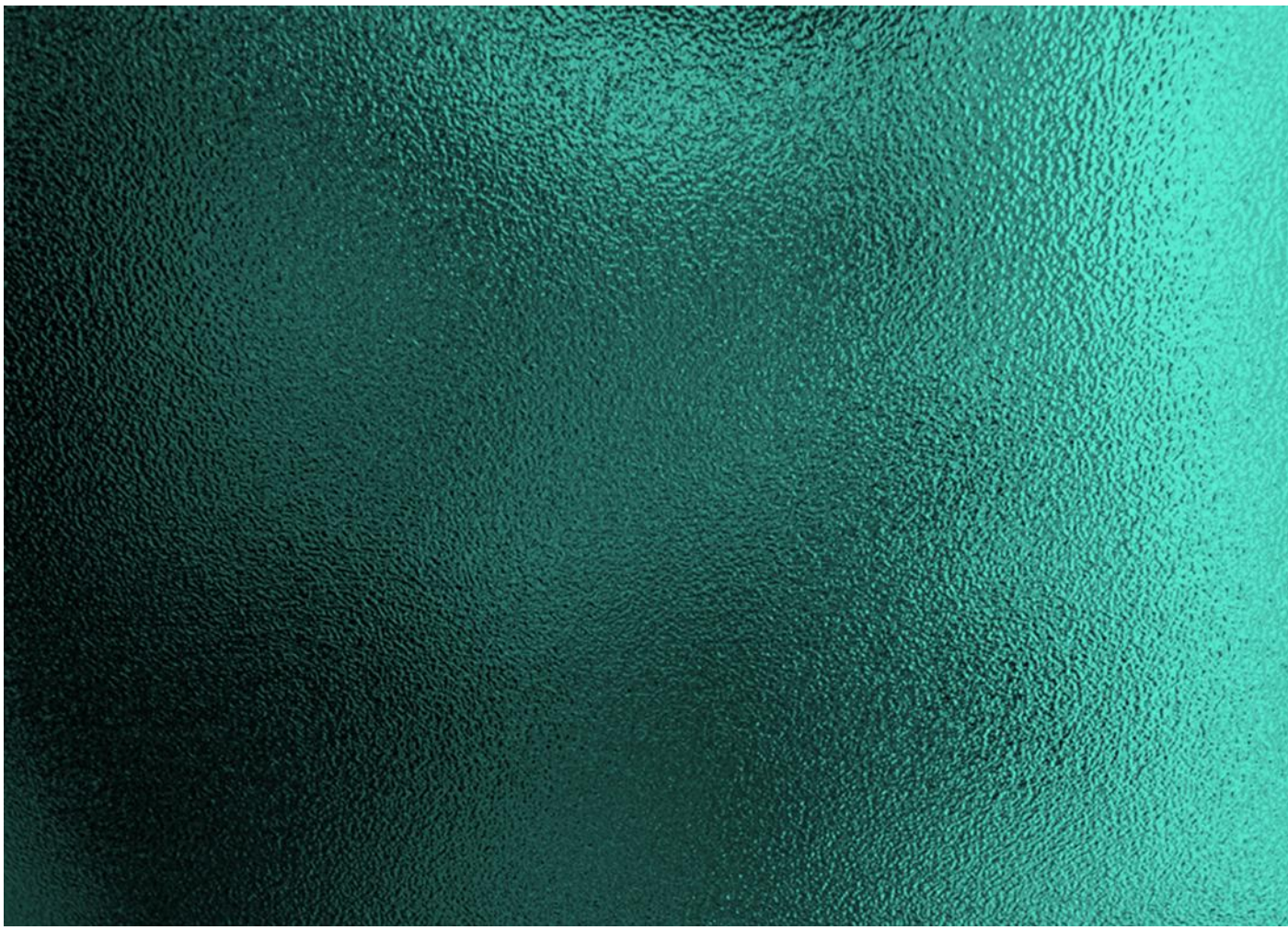
AVENTRA
SIMPLY SECURE

Security Assurance Documentation

Aventra MyEID PKI Smart Card Security Target



Version: 1.17

Purpose of the Document

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), Aventra MyEID PKI Smart Card. After the evaluation this document provides the trust to TOE's exact security properties for the targeted consumer. This Security Target (ST) defines a list of threats that the product intends to counter, a set of security objectives, a set of security requirements, the security functions provided by the TOE which meet the set of requirements and a set of assumptions about the aspects of the environment.

Document Control

Title	Aventra MyEID PKI Smart Card Security Target
Version Number	1.17
Author	Aventra Oy
Location	Kutomotie 16, 00380 Helsinki
Subject	Common Criteria EAL4+ certification
Classification	Public

Change History

Version	Date	Comments
1.0	2021-12-21	First release after Draft versions
1.1	2022-01-14	Reference changes (list of standards and footnotes)
1.2	2022-04-29	TOE version
1.3	2022-10-10	Missing information added and errors corrected after review.
1.4	2022-10-24	Completed assignments in FPT_PHP.3.1, FPT_FLS.1.1 and FDP_ITC.1.3
1.5	2024-01-17	Connected FCS_CKM.4 with SS.Secure Key Storage in the SFR to SS/SF mapping table.
1.6	2024-02-07	Added forgotten brainpoolP320r1 and brainpoolP320t1 elliptic curves.
1.7	2024-02-08	Conformance claim updated from Common Criteria for Information Technology Security Evaluation, *Version 3.1, Revision 5* to *CC:2022 Revision 1* (and template header and footer updates according to new template)
1.8	2024-06-24	- Updated platform revision to v4.7 R1.01.4 - Added note about absence of allowed-with statements in CC 3.1 based PPs. - Fixed typo FCS_COP.1.2 / Decipher -> correct is FCS_COP.1.1 / Decipher - Changed FCS_CKM.4 (because deprecated in CC:2022) to FCS_CKM.6 and updated it according to CC:2022 requirements. - Added a note about PKCS#1 padding versions under FCS_COP.1.
1.9	2024-08-21	- Added SFR FCS_CKM.3, because it is defined as a dependency for FCS_COP.1 and FCS_CKM.1 in CC:2022
1.10	2024-10-15	- Correction to description of SS.Key Wrapping: AES keys can be wrapped, ECC key cannot. - Corrections to Table 10 (SS/SF to SFR mapping): Marked missing SFRs to SS.Key Unwrapping, SS.Key Import and SS.Key Generation - Added a note under FCS_CKM.3.1 and added related standards to the list of standards. - Removed PACE from SF.Secure Messaging, because it is not supported in MyEID 5.0.0 - Corrections to platform SFRs used by the TOE

1.11	2024-10-21	- Removed FPT_EMS.1 from extended components definition, because it is defined in CC:2022 part 2. Updated the SFR definition accordingly. - Removed 3DES C/R pins from description of SS.User Authentication. This is now out of scope of certification. - Corrected incomplete marking of a selection in FDP_ACF.1.2/SVD_Transfer
1.12	2024-11-07	- Updated the platform certification report reference to a newer 4/2024 report NSCIB-CC-2300172-01-CR. - Added a reference to the newer R1.02.4 revision of the JCOP4 P71 platform. - Updated description of C/R authentication under TOE Overview and description: Triple-DES replaced with AES.
1.13	2024-12-05	- Updated the TOE description regarding platform versions. - Clarified in 1.3.1 that Triple DES is not used in the certified configuration - Updated dependencies of FCS_COP.1, FCS_CKM.1 and FCS_CKM.6 according to “Errata to CC:2022 and CEM:2022” - Update platform ST and user guidance versions in the reference list
1.14	2025-03-16	- Correction to SFRs FIA_UAU.1 and FIA_UID.1. - Corrections to 7.3. Some associations between SFRs and TSF were missing. 2025-03-16 Internal review, JS
1.15	2025-04-24	- Added FCS_CKM.6 as dependency to FCS_COP.1/AES. - Added description of delivery items under 1.2.5.1. 2025-05-14 Internal review, JS
1.16	2025-08-12	- Corrected OT.Decipher_Auth -> OT.Crypto_OP_Auth in 4.4.1 Security objectives backtracking table - Replaced an unintentionally left comment about mentioning platform protection with reference to the platform SFR table in 6.3.3 / OT.Lifecycle_Security - Added description of SFR sufficiency for OTs defined in 4.2 - Connected FC_ACF.1 with OT.Crypto_Op_Auth in security requirements coverage
1.17	2026-02-23	- Updated 2.4 Conformance Rational to mention strict conformance - Updated 1.2.2 TOE Frame: Clarified that additional/3rd part applets are ruled out in the certified TOE - Fixed typos, reorganized headings under sect. 6. - Updated OE.SVD_Auth but splitting it into two versions as described in [EUCC_SotA] - Mentioned [EUCC_SotA] in 2.2.2 - Added 6.3.3 about fulfillment of dependencies - Updated references - Improved description of TOE Life-cycle - Rewrote 2.2.1 2026-02-23 Internal review, JS

References

Common Criteria related

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CC: 2022, Revision 1, November 2022, CCMB-2022-11-001

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CC: 2022, Revision 1, November 2022, CCMB-2022-11-002

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CC: 2022, Revision 1, November 2022, CCMB-2022-11-003

[CC4] Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, CC: 2022, Revision 1, November 2022, CCMB-2022-11-004

[CC5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, CC: 2022, Revision 1, November 2022, CCMB-2022-11-005

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CEM: 2022, Revision 1, November 2022, CCMB-2022-11-006

[CC2022_EI] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1)

[SOGIS-ACM] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms
https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf

[EUCC-SotA] EUCC SCHEME STATE-OF-THE-ART DOCUMENT
Security Evaluation and Certification of Qualified Electronic Signature/Seal Creation Devices according to eIDAS Regulation (EU) 910/2014, as amended by Regulation (EU) 2024/1183
Version 1, February 2025
https://certification.enisa.europa.eu/publications/security-evaluation-and-certification-qualified-electronic-signatureseal-creation-devices_en

[TPOL] CCMC-2023-04-001, Transition Policy to CC:2022 and CEM:2022 https://www.commoncriteriaportal.org/files/ccfiles/CC2022CEM2022TransitionPolicy.pdf

TOE related

[PP2] BSI-CC-PP-0059-2009-MA-02, Protection profiles for secure signature creation device – Part 2: Device with key generation, CEN/ISSS – Information Society Standardization System, EN 419211-2:2013, 2016-06-30

[PP3] BSI-CC-PP-0075-2012-MA-01, Protection profiles for secure signature creation device – Part 3: Device with key import, CEN/ISSS – Information Society Standardization System, EN 419211-3:2013, 2016-06-30

[PP_OVRVW] EN 419211-1:2014 Protection profiles for secure signature creation devices - Part 1: Overview, 10-2014

[PST] JCOP 4 P71 Security Target Lite for JCOP 4 P71 / SE050 Rev. 4.17 — 10 December 2025, NSCIB-CC-2300172-02

[PUGM] JCOP4 P71 User Guidance and Administration Manual Version 4.7, 2025-06-24

[UGM_1] MyEID PKI Smart Card Reference Manual Version 3.0.8

Legal

[DIR] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31999L0093

Standards

[ANSI X9.62] Public Key Cryptography for the Financial Services Industry: the Elliptic Curve Digital Signature Algorithm (ECDSA)

[FIPS 186-5] Digital Signature Standard (DSS)
https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf

[FIPS197] FIPS PUB 197 Advanced Encryption Standard
https://csrc.nist.gov/publications/detail/fips/197/final

[ISO14888-3] ISO/IEC 14888-3:2018 IT Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms
https://www.iso.org/standard/76382.html

[ISO7816] ISO 7816 parts 1-15 – Smart Card Standards

[PKCS#1] PKCS #1: RSA Cryptography Specifications Version 2.2
https://datatracker.ietf.org/doc/html/rfc8017

[RFC 2437] PKCS #1: RSA Cryptography Specifications
https://datatracker.ietf.org/doc/html/rfc2437

[RFC 3447] Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1
https://datatracker.ietf.org/doc/html/rfc3447

[RFC 5652] Cryptographic Message Syntax (CMS), including PKCS #7 standard.
https://datatracker.ietf.org/doc/html/rfc5652

[RFC 1851] Request for Comments: 1851 The ESP Triple DES Transform
https://datatracker.ietf.org/doc/html/rfc1851

[RFC 5639] Request for Comments: 5639
Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation
https://www.rfc-editor.org/rfc/rfc5639

[SP800-186] NIST Special Publication 800-186
https://csrc.nist.gov/pubs/sp/800/186/final

[SP800-56A] NIST Special Publication 800-56A Revision 3: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography
https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/final

[SP800-38A] NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation, Methods and Techniques
https://csrc.nist.gov/pubs/sp/800/38/a/final

[PKCS11] PKCS #11 Specification Version 3.1
OASIS Standard, 23 July 2023
https://docs.oasis-open.org/pkcs11/pkcs11-spec/v3.1/os/pkcs11-spec-v3.1-os.html

[GP] GlobalPlatform Technology Card Specification Version 2.3.1
https://globalplatform.org/wp-content/uploads/2018/05/GPC_CardSpecification_v2.3.1_PublicRelease_CC.pdf

[PIV] NIST Special Publication 800-73-5: Interfaces for Personal Identity Verification. Parts 1 and 2.
https://csrc.nist.gov/pubs/sp/800/73/pt1/5/final
https://csrc.nist.gov/pubs/sp/800/73/pt2/5/final

Abbreviations

Common Criteria related

API	Application Programming Interface
CC	Common Criteria
CM	Configuration Management
EAL4+	Evaluation Assurance Level 4 with Augmentation(+)
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirements
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SPD	Security Problem Definition
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface

Aventra TOE related

3DES	Data Encryption Standard with 3 keys also written as Triple-DES
AC	Access Condition
AES	Advanced Encryption Standard
AID	Application Identifier
APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation One
C/R	Challenge/Response
CIV	Commercial Identity Verification
CLA	Class Byte
CRDO	Control Reference Data Object
DF	Dedicated File
ECC	Elliptic Curve Cryptography
EF	Elementary File
FCI	File Control Information
FID	File Identifier
GP	GlobalPlatform
LC	Length of APDU command data
MF	Master File
MSE	Manage Security Environment
P1/P2	APDU command parameter 1 and 2
PIN	Personal Identification Number
PIV	Personal Identity Verification
PSO	Perform Security Operation
RFU	Reserved for Future Use
SE	Security Environment
SW	Status Word
ECDH	Elliptic Curve Diffie-Hellman
eIDAS	electronic IDentification, Authentication and trust Services EU regulation

PP related

CGA	Certification Generation Application
CSP	Certification Service Provider
DTBS	Data To Be Signed
DTBS/R	Data To Be Signed or its unique representation
QSCD	Qualified Signature Creation Device
RAD	Reference Authentication Data: A PIN code or an authentication key
SCA	Signature Creation Application
SCD	Signature Creation Data. Refers to private or secret keys stored on the TOE for any cryptographic usage.
SDO	Signed Data Object
SVD	Signature Verification Data
SSCD	Secure Signature Creation Device
VAD	Verification Authentication Data

Contents

1. Introduction of the Security Target (ST)

1.1 ST and TOE Reference

ST reference	
Name	Aventra MyEID PKI Smart Card Security Target
Version	1.17
Date	2026-02-23
Author	Aventra Oy

TOE reference	
Name	Aventra MyEID PKI Smart Card
Name, abbreviated form	MyEID
Version	5.0.0
Developer	Aventra Oy
Type	Multifunctional PKI smart card and Java Card applet
Platform TOE Name	JCOP 4 P71
Platform Certification ID	NSCIB-CC-2300172-02, 2026-02-12 Certification report NSCIB-CC-2300172-02-CR
Platform Version	v4.7 R1.01.4, v4.7 R1.02.4

1.2 TOE Overview and Description

The TOE is a Java Card applet running on a specific NXP's integrated circuit designed for cryptography. The TOE consists of the Common Criteria certified IC running a JCOP4 Java Card operating system, and Aventra's MyEID Java Card applet running on top of that. The TOE is primarily used for authenticating users or devices and ensuring confidentiality of data in public key infrastructure. The main features of the TOE are calculating digital signatures, deciphering data and storing cryptographic keys in a secure way.

The TOE is used with an ISO 7816 compatible smart card reader. The smart card reader can be either with physical contacts or contactless. With contactless reader, ISO 7816 commands are transmitted via ISO 14443 interface. Software applications typically communicate with the TOE using a high-level standard API such as PKCS#11 or Microsoft CNG. These interfaces use drivers and middleware, which build APDU commands defined in ISO 7816 standard to communicate with the TOE. Software applications can also use APDU commands directly.

The cryptographic key material stored on the TOE is protected physically by the IC using various techniques such as physical memory obfuscation. The IC is designed to make gaining unauthorized access to key data as difficult as possible. Logically, access to the key material

is disabled in the Java Card software applet. No commands are exposed in the command interface, which would allow extracting RSA or ECC private keys from the card. Usage of keys for cryptographic operations is restricted with PIN codes. The card locks itself if wrong PIN is submitted too many times. PIN codes can also be used to protect sensitive data stored on the card. MyEID applet relies on the platform's implementations of cryptographic algorithms. The IC contains a crypto co-processor, which is designed to run the crypto-algorithms efficiently and securely.

The TOE consists of MyEID PKI Java Card applet that is compatible with Java Card 3.0.5 classic and GlobalPlatform 2.3 specifications. The OS provided by the underlying platform consists of Java Card virtual machine (JCVM) and runtime environment (JCRE), Crypto Lib, Config service and GlobalPlatform framework (GP) and other secure components. TOE is implemented on NXP's JCOP 4 OS that is certified according to Common Criteria (EAL6+). The TOE includes its own User Guidance documentation [UGM_1].

Reference for the Java Card JCOP 4 P71	
Certification ID:	NSCIB-2300172-02
ST Reference:	JCOP 4 P71 Security Target Lite for JCOP 4 P71 / SE050 [PST]

The TOE interacts with the NXP's JCOP 4 OS and other JCOP 4 P71 Security Target components through GP, JCVM and JCRE. Interaction with GP Framework and Config Services, JCVM and JCRE is done with GP_A and JC_A APIs using Java method calls.

The JCOP4 P71 platform is available on contact-only and dual-interface smart cards in various memory configurations. JCOP4 P71 smart cards are identified with product codes J2RXXX and J3RXXX, where J2R represents the contact-only version and J3R the dual-interface version, and XXX is replaced by the available EEPROM memory in kilobytes, e.g. J2R180. JCOP4 P71 includes IC Embedded Software (for "Configuration Banking & Secure ID") which is further configured with the SECID basic OS configuration with the RSA key generation add-on enabled to be suitable for the TOE. The TOE is available on both contact-only and dual-interface versions and can be delivered on any of the different EEPROM size options available from NXP.

The TOE features RSA and ECC algorithms. RSA covers up to 4096 bit key length, ECDSA and ECDH algorithms up to 521 bit key length. It is compatible with OpenSC open source smart card toolset, and a certified Windows minidriver is available.

The TOE includes two alternative command interfaces, which are both implementations of parts 4 and 8 of ISO 7816 standard: MyEID Native Command Interface (MyEID NCI) and PIV Command Interface (PIV CI). MyEID NCI is defined by Aventra. All functions of the TOE are accessible using MyEID NCI. The PIV CI is a subset of the interface defined in [PIV] part 2: PIV Card Application Card Command Interface. The PIV CI only contains commands to use the TOE's cryptographic operations. Personalisation of the TOE, e.g. creating authentication objects, creating cryptographic keys and loading certificates to the TOE, is always done using the MyEID NCI. The purpose of the PIV CI is to enable using the TOE in operating systems and devices which have built-in support for the PIV CI, without installing additional driver

software. Both interfaces access the same internal data, e.g., keys and certificates, on the TOE. The same security model is also used internally for both interfaces.

The TOE supports the two configurations described in the two referenced Common Criteria Protection Profiles [PP2] and [PP3] in parallel, one for the SSDC with onboard key generation (configuration 1) and one for the SSCD with key import (configuration 2).

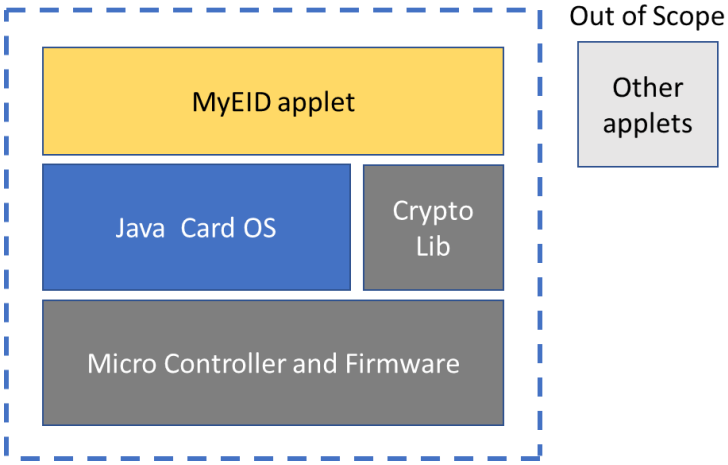
In addition to the cryptographic functionality that is defined in the protection profiles selected for this certification, the TOE includes the following cryptographic functions:

- Encipherment, decipherment and challenge/response authentication using AES algorithm
- Decipherment using RSA algorithm
- Challenge/response authentication using AES algorithm.
- Key wrapping: The TOE can use the encryption function to wrap a cryptographic key explicitly enabled for wrapping. Key wrapping is available only for symmetric keys. By default, key objects are not enabled for wrapping, and wrapping can be enabled only when a key object is created.
- Key unwrapping: The TOE can use the decryption function to unwrap a key transferred to the TOE in encrypted form and create a key object (SCD) from the decrypted key material.
- ECDH key agreement.

1.2.1 TOE Usage

The TOE is used primarily as an electronic signature creation applet in a securely managed IT environment to authenticate an individual or a device. It can also perform other cryptographic operations, e.g. data decipherment. The physical format of the TOE can vary according to the users' needs from a keyring tag to a traditional chipcard depending on available technology. The electronic signature is generated by the TOE, when the signatory provides the required authentication information.

1.2.2 TOE Frame



Picture 1. The TOE frame and modules

The blue dashed line is the boundary of the TOE. Other applets are out of scope of certification. The blue and grey boxes (Java Card OS, Crypto Library and Micro Controller and Firmware) are already CC certified modules.

MyEID Applet is an applet written in Java programming language, according to Java Card specification. Its purpose is to provide a secure interface for the outside world to communicate with the IC, and to call Java Card libraries to perform the cryptographic operations. The applet controls user authentication and manages a file system which allows organizing files, keys and authentication objects on the smart card according to ISO 7816-15 standard. The applet is loaded into the IC in Java byte code format. The communication interface to the outside world is implemented with APDU commands, as defined in ISO 7816 standard.

Java Card OS is the operating system running on the micro controller. It implements the functionality defined in the Java Card specification and communicates with the firmware or the micro controller to perform low level tasks, and with the Crypto Lib, to perform cryptographic operations. GlobalPlatform Framework, as part of the platform, manages loading applets to the card in a secure and controlled way.

Crypto Lib is a software library stored in native code of the microcontroller, which implements cryptographic algorithms and controls the crypto-coprocessor.

All components of the TOE reside in the micro controller, which is embedded in a smart card or other physical object, for example a key ring tag. The smart card can be in credit card form factor or in SIM card form factor.

The Secure IC with cryptographic library (Crypto Lib) combined with the Java Card OS comprises the platform, which is the already certified component of the TOE. The MyEID applet provides the functionality of a SSCD (or QSCD in eIDAS context) to users of the TOE and implements the TSF using services of the platform.

While the Java Card architecture allows several applets to be installed on the same smart card, the TOE in its certified configuration does not contain or allow installing other applets. Only applets which are part of the certified platform, such as the optional MIFARE applet or the Card Manager may be present besides MyEID.

1.2.3 Other Hardware and Software requirement for TOE

Requirements for TOE functionality:

- Smart card reader (compliant to ISO 7816 / ISO 14443)

1.2.4 TOE States (Life-cycle)

The life cycle of the TOE includes logical phases and technical states. The main logical phases are **Development, Production, Delivery, Personalisation** and **Operational Usage**.

In the development phase, the MyEID applet is developed by using Java programming language, JavaCard developer tools provided by the platform vendor, and a version management system. The development phase includes review of changes and new features, and testing. When a new version of the MyEID applet has passed the tests defined in the test plan, a binary bytecode package (CAP file) is built and transferred to production.

In the production phase, MyEID applet is loaded into smart cards equipped with the platform. Applet loading is done in Aventra's production facility. After the production phase, the TOE includes an empty MyEID applet which does not contain sensitive information.

In the Delivery phase the TOE is delivered to customer. The customer is typically a company or organisation, which purchases the cards in bulk.

In the Personalisation phase, the TOE is initialised with a file structure, authentication objects (RAD), cryptographic keys and certificates. Personalisation can be done in Aventra's production facility, before Delivery, or after Delivery at customer's premises. At the end of Personalisation phase, the applet is activated and the authentication objects become effective. Regardless of whether personalisation is done at Aventra or after Delivery to customer,

In the **Operational Usage** phase, the TOE is used for its purpose to perform cryptographic operations e.g., to create signatures or decrypt data. The usage phase ends when the card expires, is revoked, breaks up physically or is no longer needed.

The TOE has two (2) Main technical Life-cycle states:

- Creation State
- Operational State

Additionally, there are two more states:

- Admin State
- Global Unblocker State

An empty TOE card is in Creation State, where access conditions are not effective. This way the whole card personalisation can be completed without verifying PINs required to access

the files included in the process. After personalization, ACTIVATE APPLET command must be issued, which switches the TOE to Operational State. The only way to switch the TOE back to Creation State is to reinitialise it, which empties its contents (files, keys and PINs) completely.

Admin State and Global Unblocker State allow changing and unblocking other PINs. These features are optional properties of PINs – they cannot be used to change or unblock a PIN, unless permission for this has been granted when creating the PIN object.

In addition, there are technical states of the platform, which are relevant during delivery of the smart card bodies to Aventra and during Production phase. These states are documented in [GP], platform's user guidance and in non-public CC certification documents. They are not relevant for the user of the TOE.

The following table presents the life-cycle states of the TOE as defined in [PP1] and [PP2] and contains a mapping between the logical phases and technical states.

Table 1: TOE life-cycle phases and states

ID	Phase	Sub-phase ID	Sub-phase	Technical states	Tasks/Description
1	Development Phase	1.1	SSCD Development	not in scope of ST	Design, development and testing of the JavaCard applet
		1.2	SSCD Production	not in scope of ST	Loading applets to ICs.
2	Delivery to SSCD Provisioning Service	2.1		Creation State	Aventra can act also in the role of SSCD Provisioning service.
3	Usage Phase	3.1	SSCD Preparation	Creation State -> Operational State	Initialization of SCD, certificate request and import, personalisation for signatory. In case Aventra is the SSCD Provisioning service, this phase is done at Aventra's production site.
		3.2	Delivery to Signatory	Operational State	
		3.3	SSCD Operational use	Operational State (optional Admin State and Global Unblocker state my be active, if configured)	Authenticate Signatory, Create Signatures, Destroy SCD, Create SCD/SVD, export SVD

1.2.5 Secure Delivery of the TOE

The TOE can be delivered to the customer either before or after the Personalisation phase. In both alternatives, the MyEID applet is loaded to the smart card IC before delivery. In case the TOE is delivered without personalisation, it does not contain sensitive information such as private keys or user data. Secure delivery requires procedures, that ensure that exactly the correct version of the TOE is packaged. At the customer, the TOE must be identified according to user guidance.

In case the TOE is personalised at the vendor, it is important to deliver the VAD associated with the corresponding RAD and SCD separately. This can be done either using traditional secure PIN envelopes mailed separately or transferring the VAD digitally using a secure communication channel. It is recommended to use a mechanism, where users receive an intermediate activation VAD. After authenticating with the activation VAD, users are required to change it to a personal VAD (a PIN or a key). This way it can be noticed, if someone would have used the TOE before it is handed over to the actual user.

1.2.5.1 Delivery items

The delivery comprises the following items:

Type	Name/Description	Version	Form of delivery
Smart card	MyEID PKI Smart Card A composite product, which consists of the following non-separable sub-items: - plastic card body - NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library - JCOP4 OS - MyEID JavaCard applet	5.0.0	Trackable shipment or collected from Aventra site [1]
Document	MyEID PKI Smart Card Reference Manual	3.0.7	Electronic document[2]
Document	MyEID PKI Smart Card Reference Manual - Annex I - CC Requirements Mapping	3.0.7	Electronic document[2]
Document	MyEID PKI Smart Card - Getting Started Guide v8.2.pdf	8.2	Electronic document[2]
Public key	MyEID Factory Root Key	N/A[3]	x.509 certificate downloadable at Aventra web site
Public key	MyEID Version Signing Key for MyEID 5.0.0, Certified version	N/A[3]	x.509 certificate downloadable at Aventra web site

Please see [UGM_1] MyEID PKI Smart Card reference manual for acceptance procedure, and details of the card genuineness verification mechanism. The cryptographic card authenticity verification proves that the TOE's authentication data has been signed with private keys which are only in possession of Aventra. An important aspect of the verification is to ensure that the public keys used are obtained directly from Aventra. TOE users should verify that the verification keys or certificates are downloaded using a secure TLS connection from

[1] Authenticity of the delivered TOE can be verified cryptographically with the public keys, as described in [UGM_1]. During delivery, the TOE does not contain extractable sensitive material.
[2] Freely available for download at Aventra's web site https://aventra.fi
[3] New certificates are published on Aventra's web site, when validity period of the certificates end. Aventra publishes information how to identify, which certificate should be used to verify MyEID cards delivered at specific time.

https://aventra.fi website. The connection should be shown as trusted by the web browser. Aventra's web site uses a certificate from a well-known CA, which is usually marked as trusted by default in browsers and operating systems. In case of doubt, users are advised to contact Aventra directly.

1.3 Compatibility Statement

The TOE uses the platform's functionality to perform its security functions whereas possible, and where recommended or required in the platform's user guidance. The compatibility of the TOE's TSF with the platform's TSF is ensured as follows:

- The platform ST states that it complies with the Java Card System - Open Configuration Protection Profile, which defines the security mechanisms of the Java Card specification.
- The platform's Security Objectives for the Operational Environment are mapped to the TOE's security functions. How each objective is met is described in table "Compatibility Mapping Between this ST and the platform ST".
- Table "Platform SFRs Used by This Composite ST" describes which platform SFRs the TOE uses either to perform its security functions, and which SFRs are relevant as security features which protect the TOE.
- Platform user guidance is followed 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.

1.3.1 Platform SFRs Used by This Composite ST

The mapping between the platform SFRs and the Security Services and Features of the ST at hand already shows that there are no contradictions on this level. This also shows implicitly that no contradictions in the objectives for the TOE exist, as the SFRs are being derived from those.

The following categorization is used for marking relevance of each Platform SFR to the Composite-ST:

Table 2: Platfrom SFR Relevance Descriptions

Relevance	Description
IP_SFR	Irrelevant Platform-SFRs not being used by the Composite-ST.
RP_SFR-SERV	Relevant Platform-SFRs being used by the Composite-ST to implement a security service with associated TSFI.
RP_SFR-MECH	Relevant Platform-SFRs being used by the Composite-ST because of its security properties providing protection against attacks to the TOE as a whole and are addressed in ADV_ARC. These required security properties are a result of the security mechanisms and services that are implemented in the Platform TOE.

Table 3: Platform SFRs Used by ST

Platform SFR	Relevance	Comment
FDP_ACC.2[Firewall]	RP_SFR-MECH	general security feature of the platform protecting the TOE
FDP_ACF.1[Firewall]	RP_SFR-MECH	general security feature of the platform protecting the TOE
FDP_IFC.1[JCVM]	RP_SFR-MECH	general security feature of the platform protecting the TOE
FDP_IFF.1[JCVM]	RP_SFR-MECH	general security feature of the platform protecting the TOE
FDP_RIP.1[OBJECTS]	RP_SFR-SERV	Related to TOE SFR FDP_RIP.1, and SS.File Management
FMT_MSA.1[JCRE]	RP_SFR-MECH	A dependency of platform SFR FMT_MSA.3[FIREWALL]
FMT_MSA.1[JCVM]	IRP_SFR-MECH	A dependency of platform SFR FMT_MSA.3[FIREWALL]
FMT_MSA.2[FIREWALL-JCVM]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_MSA.3[FIREWALL]	RP_SFR-MECH	Dependency of FDP_ACF.1[FIREWALL]
FMT_MSA.3[JCVM]	RP_SFR-MECH	Dependency of platform SFR FMT_IFC.1[JCVM]
FMT_SMF.1	RP_SFR-MECH	Dependency of other platform SFRs in the same category.
FMT_SMR.1	RP_SFR-MECH	Dependency of other platform SFRs in the same category.
FCS_CKM.1	RP_SFR-SERV	Used by SS.Key Generation
FCS_CKM.3	RP_SFR-SERV	Used by SS.Key Wrapping to access the key being wrapped.

FCS_CKM.4	RP_SFR-SERV	Used by SS.File Management when key files are destroyed.
FCS_COP.1[PUF_AES]	IP_SFR	not being used by the TOE
FCS_COP.1[PUF_MAC]	IP_SFR	not being used by the TOE
FCS_COP.1[TripleDES]	RP_SFR-SERV	Not being used by the certified configuration of the TOE*
FCS_COP.1[AES]	RP_SFR-SERV	used by SS.User Authentication, SS.Data Encipherment, SS.Data Decipherment, SF.Secure Messaging
FCS_COP.1[RSACipher]	RP_SFR-SERV	used by SS.Signature Creation and SS.Data Decipherment
FCS_COP.1[ECDHPACEKeyAgreement]	RP_SFR-SERV	not being used by the TOEs
FCS_COP.1[PIV]	RP_SFR-SERV	not used by the TOE (implemented by the TOE by combining platform-provided algorithms)
FCS_COP.1[ECDH_P1363]	RP_SFR-SERV	used by SS.Key Agreement and SF.Secure Messaging
FCS_COP.1[DESMAC]	IP_SFR	not being used by the TOE
FCS_COP.1[AESMAC]	IP_SFR	not being used by the TOE
FCS_COP.1[RSASignaturePKCS1]	RP_SFR-SERV	used by SS.Signature Creation
FCS_COP.1[ECSignature]	RP_SFR-SERV	used by SS.Signature Creation
FCS_COP.1[ECAdd]	RP_SFR-SERV	used.by SF.Secure Messaging
FCS_COP.1[SHA]	IP_SFR	not being used by the TOE
FCS_COP.1[AES_CMAC]	RP_SFR-SERV	used by SF.Secure Messaging
FCS_COP.1[DAP]	RP_SFR-MECH	used when loading the TOE to the platform
FDP_RIP.1[ABORT]	RP_SFR-MECH	Ensures that deleted objects or deallocated memory areas are no longer available.
FDP_RIP.1[APDU]	RP_SFR-MECH	Ensures that deleted objects or deallocated memory areas are no longer available.
FDP_RIP.1[GlobalArray_Refined]	RP_SFR-MECH	Ensures that deleted objects or deallocated memory areas are no longer available.
FDP_RIP.1[bArray]	RP_SFR-MECH	Ensures that deleted objects or deallocated memory areas are no longer available.
FDP_RIP.1[KEYS]	RP_SFR-MECH	Ensures that deleted objects or deallocated memory areas are no longer available, related to TOE SFR FCS_CKM.6.
FDP_RIP.1[TRANSIENT]	RP_SFR-MECH	Ensures that deleted objects or deallocated memory areas are no longer available.
FDP_ROL.1[FIREWALL]	RP_SFR-MECH	general security feature of the platform protecting the TOE
FAU_ARP.1	RP_SFR-MECH	general security feature of the platform protecting the TOE
FDP_SDI.2[DATA]	RP_SFR-MECH	general security feature of the platform protecting the TOE. Associated with TOE's SFR FDP_SDI.2/Persistent.
FDP_SDI.2[SENSITIVE_RESULT]	RP_SFR-MECH	general security feature of the platform protecting the TOE
FPR_UNO.1	RP_SFR-MECH	general security feature of the platform protecting the TOE

FPT_FLS.1	RP_SFR-MECH	general security feature of the platform protecting the TOE
FPT_TDC.1	RP_SFR-MECH	general security feature of the platform protecting the TOE
FIA_ATD.1[AID]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FIA_UID.2[AID]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FIA_USB.1[AID]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_MTD.1[JCRE]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_MTD.3[JCRE]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_SMR.1[INSTALLER]	RP_SFR-MECH	general security feature of the platform protecting the TOE
FPT_FLS.1[INSTALLER]	RP_SFR-MECH	general security feature of the platform protecting the TOE
FPT_RCV.3[INSTALLER]	RP_SFR-MECH	general security feature of the platform protecting the TOE
FDP_ACC.2[ADEL]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FDP_ACF.1[ADEL]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FDP_RIP.1[ADEL]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_MSA.1[ADEL]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_MSA.3[ADEL]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_SMF.1[ADEL]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_SMF.1.1[ADEL]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_SMR.1[ADEL]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FPT_FLS.1[ADEL]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FDP_RIP.1.1[ODEL]	RP_SFR-SERV	Associated with SS.File Management and TOE SFRs FCS_CKM.6 and FDP_RIP.1
FPT_FLS.1[ODEL]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FDP_UIT.1[CCM]	RP_SFR-MECH	general security feature of the platform protecting the TOE
FDP_ROL.1[CCM]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FDP_ITC.2[CCM]	IP_SFR	Platform's internal implementation, not used directly by the TOE

FPT_FLS.1[CCM]	RP_SFR-MECH	general security feature of the platform protecting the TOE
FDP_ACC.1[SD]	RP_SFR-MECH	general security feature of the platform protecting the TOE
FDP_ACF.1[SD]	RP_SFR-MECH	general security feature of the platform protecting the TOE
FMT_MSA.1[SD]	RP_SFR-MECH	a dependency of FDP_MSA.3[SD]
FMT_MSA.3[SD]	RP_SFR-MECH	a dependency of FDP_ACF.1[SD]
FMT_SMF.1[SD]	RP_SFR-MECH	Platform's internal implementation. Related to applet loading and management, but not used directly by the TOE. A dependency of FMT_MSA.1[SD]
FMT_SMR.1[SD]	RP_SFR-MECH	Platform's internal implementation. Related to applet loading and management, but not used directly by the TOE. A dependency of FMT_MSA.3[SD]
FCO_NRO.2[SC]	IP_SFR	Platform's internal implementation. Related to applet loading and management, but not used by the TOE itself.
FDP_IFC.2[SC]	IP_SFR	Platform's internal implementation. Related to applet loading and management, but not used by the TOE itself.
FDP_IFF.1[SC]	IP_SFR	Platform's internal implementation. Related to applet loading and management, but not used by the TOE itself.
FMT_MSA.1[SC]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_MSA.3[SC]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_SMF.1[SC]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FIA_UID.1[SC]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FIA_UAU.1[SC]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FIA_UAU.4[SC]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FTP_ITC.1[SC]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FDP_ACC.1[EXT-MEM]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FDP_ACF.1[EXT-MEM]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_MSA.1[EXT-MEM]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_MSA.3[EXT-MEM]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_SMF.1[EXT-MEM]	IP_SFR	Platform's internal implementation, not used directly by the TOE

FDP_IFC.2[CFG]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FDP_IFF.1[CFG]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_MSA.3[CFG]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_MSA.1[CFG]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_SMR.1[CFG]	IP_SFR	Platform's internal implementation, not used directly by the TOE
MT_SMF.1[CFG]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FIA_UID.1[CFG]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FDP_ACC.2[SecureBox]	IP_SFR	The TOE does not use the platform's SecureBox functionality
FDP_ACF.1[SecureBox]	IP_SFR	The TOE does not use the platform's SecureBox functionality
FMT_MSA.1[SecureBox]	IP_SFR	The TOE does not use the platform's SecureBox functionality
FMT_MSA.3[SecureBox]	IP_SFR	The TOE does not use the platform's SecureBox functionality
FMT_SMF.1[SecureBox]	IP_SFR	The TOE does not use the platform's SecureBox functionality
FDP_IFC.1[MODULAR-DESIGN]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FDP_IFF.1[MODULAR-DESIGN]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FIA_ATD.1[MODULAR-DESIGN]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FIA_USB.1[MODULAR-DESIGN]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_MSA.1[MODULAR-DESIGN]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_MSA.3[MODULAR-DESIGN]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_SMF.1[MODULAR-DESIGN]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FMT_SMR.1[MODULAR-DESIGN]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FPT_FLS.1[MODULAR-DESIGN]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FIA_UID.1[MODULAR-DESIGN]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FDP_ACC.2[RM]	RP_SFR-MECH	Restricted mode operation is related to, and supports TOE's SFR FPT_PHP.3 and SF.Applet Hardening

FDP_ACF.1[RM]	RP_SFR-MECH	Restricted mode operation is related to, and supports TOE's SFR FPT_PHP.3 and SF.Applet Hardening
FMT_MSA.3[RM]	RP_SFR-MECH	Restricted mode operation is related to, and supports TOE's SFR FPT_PHP.3 and SF.Applet Hardening
FMT_MSA.1[RM]	RP_SFR-MECH	Restricted mode operation is related to, and supports TOE's SFR FPT_PHP.3 and SF.Applet Hardening
FMT_SMF.1[RM]	RP_SFR-MECH	Restricted mode operation is related to, and supports TOE's SFR FPT_PHP.3 and SF.Applet Hardening
FIA_UID.1[RM]	RP_SFR-MECH	Restricted mode operation is related to, and supports TOE's SFR FPT_PHP.3 and SF.Applet Hardening
FIA_UAU.1[RM]	RP_SFR-MECH	Restricted mode operation is related to, and supports TOE's SFR FPT_PHP.3 and SF.Applet Hardening
AU_SAS.1[SCP]	IP_SFR	Platform's internal implementation, not used directly by the TOE
FCS_RNG.1	RP_SFR-MECH	RNG quality metrics are related to FCS_CKM.1 and this provides to ensuring quality of random numbers.
FCS_RNG.1[HDT]	RP_SFR-MECH	RNG quality metrics are related to FCS_CKM.1 and this provides to ensuring quality of random numbers.
FIA_AFL.1[PIN]	RP_SFR-SERV	Related to SS.User Authentication and FIA_AFL.1 in TOE ST
FPT_EMSEC.1	RP_SFR-SERV	Related to, and supports TOE'S SFRs FPT_EMS.1. and SF.Applet Hardening
FPT_PHP.3	RP_SFR-SERV	Related to, and supports TOE's SFR FPT_PHP.3 and SF.Applet Hardening
FCS_CKM.2	PR_SFR_SERV	Related to SS.Key Import
FCS_CKM.3	RP_SFR-SERV	Used by FCS_COP.1, SS.Signature Creation, SS.Data Decipherment, SS.Data Encipherment, SS. Key Wrapping, SS.Key Unwrapping, SS.Secure Messaging.

*While Triple-DES based challenge/response authentication is supported by the TOE, this feature is out of scope of the certified functionality. This is mentioned in the user guidance.

1.3.2 Compatibility Mapping Between This ST and the Platform ST

The assumptions, security objectives for the operational environment, threats and organisational security policies defined in the platform ST are examined in this section. Their relationship to this ST is mapped in the following tables.

1.3.2.1 Platform's assumptions

The author of the ST has examined that the above-mentioned assumptions have no contradictions with the platform's assumptions. No contradictions with the TOE and the platform's assumption were found either.

Compliance with the platform's assumptions is considered in the following table:

Table 4: Platform assumption mappings

Platform assumption	Comment / remark
A.APPLET *Applets without Native Methods*	The TOE does not contain native methods and is not able to call native methods of the platform.
A.VERIFICATION *Bytecode Verification*	Bytecode verification is part of the build process and a required step in a checklist.
A.USE_DIAG *Usage of TOE's Secure Communication Protocol by OE*	Secure communication protocols are used when loading the applet. While secure communication is not technically required for users of the applet because of backward-compatibility reasons, significance of using secure communication for EAL4+ compliance is mentioned in the user guidance.
A.USE_KEYS *Protected Storage of Keys Outside of TOE*	Protected storage of keys is implemented as required by the platform assumption and user guidance. This is documented in the ALC-document class.
A.PROCESS-SEC-ID *Protection during Packaging, Finishing and Personalisation*	Compliance with this assumption has been ensured, and is documented in documentation of the production and delivery process (ALC-documents).
A.APPS-PROVIDER *Application Provider*	Developer of the TOE is in role of Application Provider. APSD keys are protected as required (ALC-documents)
A.VERIFICATION-AUTHORITY *Verification Authority*	This assumption applies to the TOE as well as to the platform.

1.3.2.2 Platform's Security Objectives for the Operational Environment

Table 5: Platform Security Objectives for Operational Environment

Security Objectives for the Operational Environment	Comment / remark
OE.APPLET *Applet*	The TOE does not use native methods. No other applet is allowed on the certified TOE.
OE.VERIFICATION *Bytecode Verification*	The TOE fulfills this requirement. Byte code verification is done using platform provider's tools. No other applet is allowed on the certified TOE.
OE.CODE-EVIDENCE *Code Evidence*	The TOE fulfills this requirement. The requirement is taken into account in the development process. No other applet is allowed on the certified TOE.
OE.APPS-PROVIDER *Application Provider*	The TOE fulfils this requirement. Secure mechanism to handle and store the security domain keys is in place. No other applet is allowed on the certified TOE.
OE.VERIFICATION-AUTHORITY *Verification Authority*	The TOE fulfils this requirement. A code signing certificate from a publicly trusted CA is used to sign the applet binaries.
OE.KEY-CHANGE Security Domain Key Change	The TOE fulfils this requirement. Procedure to change the key after loading the applet is in place.
OE.SECURITY-DOMAINS *Security Domains*	The TOE fulfils this requirement. Applet loading in post-issuance mode is not allowed in the certified TOE.
OE.USE_DIAG Secure *TOE communication protocols*	The TOE fulfils this requirement. Ensured by technical means where possible, and instructed in the user guidance.
OE.USE_KEYS *Protection of OPE keys*	The TOE fulfils this requirement. Instructed in the user guidance.
OE.PROCESS_SEC_IC *Protection during composite product manufacturing*	The TOE fulfils this requirement. Documented protections are in place in Aventra's production. Instructions on how to protect confidentially until handover to the card holder are in the user guidance.

1.3.2.3 Platform threats

The threats defined in the Platform ST were examined. No contradictions with the threats defined for the TOE were found. The platform's threats which are directly related to the TOE's threats are marked in the table below. The rest of the threats target the platform in more generic way from the TOE's perspective.

Table 6: Platform threats

Threat	Comment / Remark
T.CONFID-APPLI-DATA *Confidentiality of Application Data*	Related to T.SCD_Divulg,
T.CONFID-JCS-CODE *Confidentiality of Java Card System Code*	none
T.CONFID-JCS-DATA *Confidentiality of Java Card System Data*	No contradictions Related to T.SCD_Divulg
T.INTEG-APPLI-CODE *Integrity of Application Code*	Related to T.SCD_Divulg, T.SigF_Misuse and t.CryptF_Misuse
T.INTEG-APPLI-CODE.LOAD *Integrity of Application Code - Load*	This threat is related to the TOE's production process. The threat is countered by security measures documented in ALC-documents and by compliance with platform's user guidance.
T.INTEG-APPLI-DATA[REFINED] *Integrity of Application Data*	Related to T.SCD_Divulg.
T.INTEG-APPLI-DATA.LOAD *Integrity of Application Data - Load*	Threat countered in the TOE's production process. Documented in ALC_ documents.
T.INTEG-JCS-CODE *Integrity of Java Card System Code*	This threat is related to T.SCD_Divulg, T.SigF_Misuse and t.CryptF_Misuse
T.INTEG-JCS-DATA *Integrity of Java Card System Data*	none
T.SID.1 *Subject Identification 1*	Related to T.SCD_Divulg, T.SigF_Misuse and t.CryptF_Misuse
T.SID.2 *Subject Identification 1*	Related to T.SCD_Divulg, T.SigF_Misuse and t.CryptF_Misuse
T.EXE-CODE.1 *Code Execution 1*	none
T.EXE-CODE.2 *Code Execution 2*	none
T.NATIVE *Native Code Execution*	none
T.MODULE_EXEC *Code Execution of Modules*	none
T.RESOURCES *Consumption of Resources*	none
T.UNAUTHORIZED_CARD_MNGT *Unauthorized Card Management*	This threat is related to the TOE's production process. The threat is countered by security measures documented in ALC-documents and by compliance with platform's use guidance.
T.COM_EXPLOIT *Communication Channel Remote Exploit*	Related to T.SCD_Divulg, T.SigF_Misuse and t.CryptF_Misuse
T.LIFE_CYCLE *Life Cycle*	none
T.OBJ-DELETION	none

Object Deletion	
T.PHYSICAL *Physical Tampering*	Related to T.Hack_Phys
T.OS_OPERATE *Incorrect Operating System Behavior*	none
T.RND *Deficiency of Random Numbers*	Related to T.SCD_Derive and T.Sig_Forgery, as proper implementation of the supported cryptographic algorithms require a cryptographic quality random number generator.
T.CONFIG *Unauthorized configuration*	none
T.SEC_BOX_BORDER *SecureBox Border Infringement*	Not directly relevant, as the TOE does not use the SecureBox functionality.
T.MODULE_REPLACEMENT *Replacement of Module*	none
T.ATTACK-COUNTER	none

1.3.2.4 Platform Organisational Security Policies

The organisational security policies listed in the platform ST are examined in the following table. No contradictions with the TOE ST were found.

Table 7: Platform OSPs

Organisational Security Policy	Comment / remark
OSP.VERIFICATION *File Verification*	This OSP is addressed in [PUGM] and implemented as instructed in TOE's development and production process.
OSP.PROCESS-TOE *Identification of the TOE*	The TOE has its of identification mechanism described in [UGM_1], which is used to identify the composite TOE. The platform's identification is documented in [PUGM].
OSP.KEY-CHANGE *Security Domain Key Change*	This OSP is addressed in [PUGM] and implemented as instructed in TOE's production process.
OSP.SECURITY-DOMAINS *Security Domains*	This OSP is addressed in [PUGM] and implemented as instructed in TOE's production process.
OSP.SECURE-BOX *Secure Box Border*	The TOE does not use the platform's Secure Box Functionality.

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 CC2022 R1 according to:

- "Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CC: 2022, Revision 1, November 2022, CCMB-2022-11-001" [CC1]
- "Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CC: 2022, Revision 1, November 2022, CCMB-2022-11-002" [CC2]
- "Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CC: 2022, Revision 1, November 2022, CCMB-2022-11-003" [CC3]
- "Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities, CC: 2022, Revision 1, November 2022, CCMB-2022-11-004" [CC4]
- "Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements, CC: 2022, Revision 1, November 2022, CCMB-2022-11-005" [CC5]
- "Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CEM: 2022, Revision 1, November 2022, CCMB-2022-11-006" [CEM]

This Security Target claims to be CC Part 2 [CC2] and CC Part 3 conformant.
The methodology "Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CEM: 2022, Revision 1 " [CEM] will be used for the evaluation.

2.2 PP Conformance Claim

This Security Target claims strict conformance with:

- BSI-CC-PP-0059-2009-MA-02, Protection profiles for secure signature creation device – Part 2: Device with key generation, CEN/ISSS – Information Society Standardization System, EN 419211-2:2013, 2016-06-30 [PP2]
- BSI-CC-PP-0075-2012-MA-01, Protection profiles for secure signature creation device – Part 3: Device with key import, CEN/ISSS – Information Society Standardization System, EN 419211-3:2013, 2016-06-30 [PP3]

More specifically: Strict conformance with [PP2] is claimed when the TOE is configured with generated keys and strict conformance with [PP3] is claimed when the TOE is configured with imported keys. Both configurations can exist in parallel in a single instance of the TOE.

2.2.1 CC:2022 transition note

The PPs this ST claims conformance with are based on CC version 3.1 R5. Aventra follows the CC3.1 to CC:2022 transition policy as defined in [TPOL].

2.2.2 Protection Profiles claimed at the same time

Some inconsistencies and problems when combining [PP2] and [PP3] within a “strict conformance” claim of a ST in a single product certification have been observed. These problems, and some inconsistencies within a single PP have been addressed in [EUCC_SotA]. This ST takes into account and follows the guidance included in this document.

2.3 Package Claim

This Security Target claims conformance with assurance package EAL4 augmented with AVA_VAN.5

- AVA_VAN.5: Advanced methodical vulnerability analysis

The platform claims conformance to the assurance package EAL6. The augmentation to EAL6 is ASE_TSS.2 “TOE summary specification with architectural design summary” and ALC_FLR.1 “Basic flaw remediation”. The Composite TOE assurance requirements of the EAL4 package are a subset of the platform EAL6 package. For augmentation AVA_VAN.5 the platform ST claims the same level.

2.4 Conformance Rational

This ST strictly conforms to all elements in both PPs.

3 Security problem definition

Assets, users, threat agents (3.1) and threats (3.2) are taken from the PPs. The TOE has security functions which are not fully covered by the PPs: Data encipherment, data decipherment, key agreement, key wrapping and key unwrapping. The definitions have been extended to cover these security features.

3.1 Assets, users, and threat agents

Assets and objects:

a) SCD: private key used to perform cryptographic operations: electronic signature generation, ECDH key agreement, data decipherment and key unwrapping. The confidentiality, integrity, and signatory’s sole control over the use of the SCD shall be maintained.
b) 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.
c) 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.

Users and subjects acting for users:

a) 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.

b) 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.
c) 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.

Threat agents:

a) 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.

3.2 Threats

3.2.1 ***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.

3.2.2 ***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.

3.2.3 ***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.

3.2.4 ***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.

3.2.5 ***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.

3.2.6 ***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.

3.2.7 ***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.

3.2.8 ***T.CryptF_Misuse*** *Unauthorised use of cryptographic functions*

An attacker gains unauthorised access to key agreement, encipherment or decipherment function of the TOE, or indirectly feeds forged data to these functions with intention to gain knowledge of the SCD or enciphered data.

This threat is not included in the selected PPs.

3.3 *Organisational security policies*

Organisation Security Policies are taken from the PP.

3.3.1 ***P.CSP_QCert*** *Qualified certificate (In blue additionally written in [PP2])*

The CSP uses a trustworthy CGA to generate a qualified certificate or non-qualified certificate (cf. **the Directive** [DIR], article 2, Clause 9, and Annex I) 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.

3.3.2 ***P.QSign*** *Qualified electronic signatures*

The signatory uses a signature creation system to sign data with an advanced electronic signature (cf. **the Directive** [DIR], article 1, Clause 2), which is a qualified electronic signature if it is based on a valid qualified certificate (according to **the Directive** [DIR] Annex I)[4]. 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.

3.3.3 ***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.

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

3.3.4 ***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.

3.4 Assumptions

3.4.1 ***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.

3.4.2 ***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.

3.4.3 ***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:

4.1.1 ***OT.Lifecycle_Security*** *Lifecycle security [PP2 / PP3]*

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

4.1.2 ***OT.SCD/SVD_Auth_Gen*** *Authorised SCD/SVD generation [PP2]*

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

4.1.3 ***OT.SCD_Auth_Imp*** *Authorised SCD import [PP3]*

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

4.1.4 ***OT.SCD_Unique*** *Uniqueness of the signature creation data [PP2]*

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.

4.1.5 ***OT.SCD_SVD_Corresp*** *Correspondence between SVD and SCD [PP2]*

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.

4.1.6 ***OT.SCD_Secrecy*** *Secrecy of the signature creation data. [PP2 / PP3]*

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

4.1.7 ***OT.Sig_Secure*** *Cryptographic security of the electronic signature [PP2 / PP3]*

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.

4.1.8 ***OT.Sigy_SigF*** *Signature creation function for the legitimate signatory only [PP2 / PP3]*

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

4.1.9 ***OT.DTBS_Integrity_TOE*** *DTBS/R integrity inside the TOE [PP2 / PP3]*

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.

4.1.10 ***OT.EMSEC_Design*** *Provide physical emanations security [PP2 / PP3]*

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

4.1.11 ***OT.Tamper_ID*** *Tamper detection [PP2 / PP3]*

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

4.1.12 ***OT.Tamper_Resistance*** *Tamper resistance [PP2 / PP3]*

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

4.2 Security Objectives not included in the Protection Profiles

The following security objectives are related to functionality of the TOE which is not included in the selected PPs.

4.2.1 ***OT.Key_Agreement_Security*** *Cryptographic security of the shared secret*

The key agreement function shall generate cryptographically secure shared secrets, which cannot be discovered with publicly known data, or data extracted from the TOE. SCD shall not be reconstructable using the shared secret.

4.2.2 ***OT.Secure_Encipherment*** *Cryptographic security of enciphered data*

The encipherment function shall encipher data in cryptographically secure way, conforming to AES algorithms specification.

4.2.3 ***OT.Crypto_Op_Auth*** *Cryptographic operations enabled only for authorized user*

Cryptographic operations such as decipherment, key agreement, key wrapping and key unwrapping, which require using a cryptographic key (SCD) stored on the TOE, shall be available only for an authenticated user authorized to use the selected key. Usage of the key shall be restricted with security attributed access control.

4.3 Security Objectives for the Operational Environment

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

4.3.1 ***OE.SVD_Auth*** *Authenticity of the SVD [PP2]*

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.

4.3.2 ***OE.SVD_Auth*** *Authenticity of the SVD [PP3]*

The operational environment shall ensure the authenticity 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.

4.3.3 ***OE.CGA_QCert*** *Generation of qualified certificates [PP2 / PP3]*

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.

4.3.4 ***OE.SSCD_Prov_Service*** *Authentic SSCD provided by SSCD-provisioning service [PP2 / PP3]*

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.

4.3.5 ***OE.HID_VAD*** *Protection of the VAD [PP2 / PP3]*

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.

4.3.6 ***OE.DTBS_Intend*** *SCA sends data intended to be signed [PP2 / PP3]*

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.

4.3.7 ***OE.DTBS_Protect*** *SCA protects the data intended to be signed [PP2 / PP3]*

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.

4.3.8 ***OE.Signatory*** *Security obligation of the signatory [PP2 / PP3]*

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:

4.3.9 ***OE.SCD/SVD_Auth_Gen*** *Authorised SCD/SVD generation [PP3]*

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

4.3.10***OE.SCD_Secrecy*** *SCD Secrecy [PP3]*

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.

*4.3.11 **OE.SCD_Unique** Uniqueness of the signature creation data [PP3]*

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.

*4.3.12 **OE.SCD_SVD_Corresp** Correspondence between SVD and SCD [PP3]*

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.

4.4 Security Objectives Rationale

4.4.1 Security objectives backtracking

Table 8: Mapping of security problem definition to security objectives

The security objects and problem with gray background are not included in the selected PPs.

Security Objects / Security problem definition (threats, organisational policies and assumptions)	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen [PP2]	OT.SCD_Auth_Imp [PP3]	OT.SCD_Unique [PP2]	OT.SCD_SVD_Corresp [PP2]	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.Key_Agreement_Security	OT.Secure_Encipherment	OT.Crypto_Op_Auth	OE.SVD_Auth [PP2]	OE.SVD_Auth [PP3]	OE.CGA_QCert	OE.SSCD_Prov_Service	OE.HID_VAD	OE.DTBS_Intend	OE.DTBS_Protect	OE.Signatory	OE.SCD/SVD_Auth_Gen [PP3]	OE.SCD_Secrecy [PP3]	OE.SCD_Unique [PP3]	OE.SCD_SVD_Corresp [PP3]
T.SCD_Divulg			X			X																		X	X		
T.SCD_Derive		X					X																			X	
T.Hack_Phys						X				X	X	X															
T.SVD_Forgery [PP2]					X											X											X
T.SVD_Forgery [PP3]																	X										
T.SigF_Misuse	X							X	X											X	X	X	X				
T.DTBS_Forgery									X												X	X					
T.Sig_Forgery				X			X											X								X	
T.CryptF_Misuse													X	X	X								X			X	
P.CSP_Qcert	X		X		X													X						X			X
P.Qsign							X	X										X			X						
P.Sigy_SSCD	X	X	X	X		X	X	X	X	X		X							X					X	X	X	
P.Sig_Non-Repud	X		X	X	X	X	X	X	X	X	X	X				X	X	X	X		X	X	X		X	X	X
A.CGA																X	X	X									
A.SCA																					X						
A.CSP [PP3]																								X	X	X	X

4.4.2 Security objectives sufficiency

Countering of threats by security objectives:

T.SCD_Divulg (Storing, copying and releasing of the signature creation data) deals with the threat of an attacker storing or coping the SCD outside the TOE. This attack is being countered by OT.SCD_AUTH_IMP [PP3] by limiting the invocation of import of SCD to authorized users; by OT.SCD_Secrecy by securing the SCD against attacks with high attack

potential. Furthermore, this attack is countered by OE.SCD/SVD_Auth_Gen which limits the generation of SCD outside of the TOE to authorised users. Finally, OE.SCD_Secrecy contributes to countering this threat by protecting the confidentiality of the SCD during generation and export to the TOE.

T.SCD_Derive (Derive the signature creation data) describes the threat of attacker deriving the SCD from publicly known data. This threat is being countered by OT.SCD_Unique and OE.SCD_Unique, which ensure that a cryptographically secure method is used to generate the SCD. This includes using correct implementation of the SCD generation algorithm to ensure that the SCD occurs in practice only once and is not reconstructible from the SCD. OT.Sig_Secure also counters this threat by ensuring cryptographic strength of the digital signatures created with the SCD.

T.Hack_Phys (Exploitation of physical vulnerabilities) deals with an attacker interacting physically with the TOE to exploit vulnerabilities. This threat is being countered with OT.EMSEC_Design, which controls production of intelligible emanations during the TOE's operation and keeps them within safe limits. OT.Tamper_ID adds to the protection with the requirement to implement features to detect physical tampering of the TOE's components, and react to possible tampering by limiting usage of the TOE and activating protections. Furthermore, OT.Tamper_Resistance requires the TOE to prevent or resist physical tampering with specified system devices and components. The ST of the platform includes security objectives which counter the physical attacks in more detailed level, and the TOE relies also to these objectives.

T.SVD_Forgery (Forgery of the signature verification data) [PP2] 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 [PP2] that ensures the integrity of the SVD exported by the TOE to the CGA.

T.SVD_Forgery (Forgery of the signature verification data) [PP3] 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 [PP3] that ensures the authenticity of the SVD given to the CGA of the CSP.

T.SigF_Misuse (Misuse of the signature creation function of the TOE) 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 or the directive [DIR]. OT.Lifecycle_Security (Lifecycle security) requires the TOE to detect flaws during the initialisation, personalisation 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 and OE.DTBS_Protect counters manipulation of the DTBS during transmission over the channel between the SCA and the TOE. T.DTBS_Integrity_TOE (DTBS/R integrity inside the TOE) prevents the DTBS/R from alteration inside the TOE. If the SCA provides a human interface for user authentication, OE.HID_VAD (Protection of the VAD) provides confidentiality and integrity of the VAD as needed by the authentication method employed. 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.

T.DTBS_Forgery (Forgery of the DTBS/R) 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 cannot be altered in transit between the SCA and the TOE. The TOE counters this threat by the means of OT.DTBS_Integrity_TOE by ensuring the integrity of the DTBS/R inside the TOE.

T.Sig_Forgery (Forgery of the electronic signature) 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 and 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.

T.CryptF_Misuse (Unauthorised use of cryptographic functions) addresses the threat of misuse of the TOE's cryptographic functions: key agreement, data decipherment, key wrapping and key unwrapping. The misuse involves gaining unauthorized access to use these functions, and feeding forged data to these functions indirectly, with the intention of gaining knowledge of the private or secret keys. Security objectives OT.Key_Agreement_Security and OT.Secure_Encipherment address this threat by requiring using algorithms and implementations which do not leak information about the private or secret keys used in the operations. OE.SCD_Unique takes part in fulfilling these objectives, because using SCDs which are not truly unique could potentially allow attackers to gain knowledge of the SCD by for example finding relationships in enciphered data or results of key agreement operations. OT.Crypto_Op_Auth ensures that only authorized users can use these functions. OE.Signatory ensures that the signatory checks that an SCD (secret or private key in this context) 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.

Enforcement of OSPs by security objectives:

P.CSP_QCert (CSP generates qualified certificates) requires CSP to use a trustworthy CGA to generate qualified certificates and requires the CSP to ensure that the user of the TOE as SSCD is evident with signatures through the certificate or other publicly available information.

- OT.Lifecycle_Security, which requires the TOE to detect flaws during the initialisation, personalisation and operational usage;
- OT.SCD_SVD_Corresp, which requires to ensure the correspondence between the SVD and the SCD during their generation;
- 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 (Qualified electronic signatures) 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 (TOE as secure signature creation device) requires the TOE to meet Annex III of the Directive [DIR]. This is ensured as follows:

- OT.SCD_Unique meets the paragraph 1(a) of Annex III, 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 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_Secrecy and OT.Sig_Secure meet the requirement in paragraph 1(b) of Annex III by the requirements 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 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 as the TOE shall not alter the DTBS/R.

Paragraph 2 of Annex III, 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, personalisation and operational usage;

- OT.SCD/SVD_Auth_Gen, which limits invocation of the generation of the SCD and the SVD to authorized 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.

OE.SSCD_Prov_Service ensures that the signatory obtains an authentic copy of the TOE, initialised and personalised SSCD from an SSCD-provisioning service.

P.Sig_Non-Repud (Non-repudiation of signatures) 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.SSCD_Prov_Service ensures that the signatory obtains an authentic copy of the TOE, initialised and personalised as SSCD from the SSCD-provisioning service.
OE.CGA_QCert ensures that the certificate allows to identify the signatory and thus to link the SVD to the signatory. OE.SVD_Auth [PP2/PP3] 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 SSCDprovisioning 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, OE.DTBS_Protect 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.

Upkeep of assumptions by security objectives:

A.SCA (Trustworthy signature creation application) is fulfilled by OE.DTBS_Intend, 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. In practice fulfilment of this assumption is ensured with user guidance, by instructing users to use only trusted, digitally signed SCA's, and ensuring they are from a trusted vendor.

A.CGA (Trustworthy certificate generation application) 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 [PP2/PP3] (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.

5 Extended Components Definition

This Security Target does not include extended components.

6 Security Requirements

6.1 Security Functional Requirements

6.1.1 Use of requirement specifications

ISO/IEC 15408 allows several operations to be performed on functional requirements; *refinement*, *selection*, *assignment*, and *iteration*. Each of these operations is used in [PP1] and [PP2]. Operations not performed in [PP1] or [PP2] are identified in order to enable instantiation of the [PP1] and [PP2] into this Security Target (ST).

A **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is (i) denoted by the word "refinement"

in **bold** text and the added or changed words are in **bold** text, or (ii) included in text as bold text and marked by a footnote. In cases where words from a CC requirement were deleted, a separate attachment indicates the words that were removed.

A **selection** operation is used to select one or more options provided by the CC in stating a requirement. A selection that has been made in this European Standard is indicated as underlined text and the original text of the component is given by a footnote. Selections left to be filled in by the ST author appear in square brackets with an indication that a selection is to be made, [selection:], and are *italicised*.

An **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment that that has been made in this European Standard is indicated as underlined text and the original text of the component is given by a footnote. Assignments filled by the ST author are in **bold** text to distinguish them from the assignments already completed in the PP. In the footnotes associated with the assignments filled by the ST author, the value to be assigned is *italicised*.

An **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing a slash "/", and the iteration indicator after the component identifier.

6.1.2 SFRs not included in Protection Profiles

The TOE includes security functions, based on security objectives to counter threats, which are not included in the selected protection profiles. The SFR's defined in this section, which refer to Signature Creation Function, apply to all cryptographic operations that can be performed by the TOE: Data encipherment and decipherment, key agreement, key wrapping and unwrapping. The security controls are implemented to protect usage of a cryptographic key, referred to as SCD, in any operation, and the same implementation is used regardless of the operation.

6.1.3 Cryptographic support (FCS)

*6.1.3.1 **FCS_CKM.1 / ECC** Cryptographic key generation*

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction

FCS_CKM.1.1 / ECC	The TSF shall generate an **SCD/SVD pair** in accordance with a specified cryptographic key generation algorithm **ECDSA (ECC over GF(p)) key generation**[5] and specified cryptographic key sizes **ECC 256, 320, 384, 512, 521 bit**[6] that meet the following: **ISO/IEC 14888-3, ANSI X9.62, [SP800-186], [RFC 5639] and [FIPS 186-5]** [7]

Note: FCS_CKM.1 / ECC relies on the platform SFR FCS_RNG.1 to fulfil this dependency.

[5] [assignment: *cryptographic key generation algorithm*]
[6] [assignment: *cryptographic key sizes*]
[7] [assignment: *list of standards*]

6.1.3.2 ***FCS_CKM.1 / RSA*** *Cryptographic key generation*

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_CKM.5 Cryptographic key derivation, or FCS_COP.1 Cryptographic operation] [FCS_RBG.1 Random bit generation, or FCS_RNG.1 Generation of random numbers] FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_CKM.1.1 / RSA	The TSF shall generate an **SCD/SVD pair** in accordance with a specified cryptographic key generation algorithm **RSA key generation**[8] that meet the following: [**FIPS 186-5]**[9]**.** The following cryptographic key sizes are supported: **between 3008 to 4096 bits in 64 bit increments**[10] are supported.
Note:	FCS_CKM.1 / RSA relies on the platform SFR FCS_RNG.1 to fulfil this dependency.

6.1.3.3 ***FCS_CKM.3*** *Cryptographic key access*

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 or FCS_CKM.5 Cryptographic key derivation]
	FCS_CKM.3.1 The TSF shall perform **extraction of AES keys for cryptographic key backup, cryptographic key archival, cryptographic key escrow, and cryptographic key recovery or transferring cryptographic keys to another system or storage**[11] accordance with a specified cryptographic key access method: **key wrapping**[12] that meets the following: **[PKCS11], [FIPS197], [SP 800-38A], [RFC 5652]** [13]**.**

[8] [assignment: cryptographic key generation algorithm]
[9] [assignment: list of standards]
[10] [assignment: cryptographic key sizes]
[11] [assignment: type of cryptographic key access]
[12] [assignment: cryptographic key access method]
[13] [assignment: list of standards]

Note: FCS_CKM.3.1 is applicable only for AES keys. RSA and ECC keys cannot be extracted from the TOE.

Note 2: The TOE's implementation of key wrapping uses the AES algorithms and is designed for implementing C_WrapKey function of the PKCS#11 standard with mechanisms CKM_AES_ECB, CKM_AES_CBC and CKM_AES_CBC_PAD.
[SOGIS-ACM] recommends using specified mechanisms with Authenticated Encryption for key wrapping. The TOE's implementation does not include AE. Integrity of wrapped keys shall be ensured by other means. The preferred method is calculating and verifying a Key Check Value with the method specified in [GP].

*6.1.3.4 **FCS_CKM.6** Timing and event of 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, or FCS_CKM.5 Cryptographic key derivation]
FCS_CKM.6.1	The TSF shall destroy **RSA, ECC and AES keys (including keying material)**[14] when no longer needed[15], when explicitly requested using SS.File Management TSF and upon re-initialising the applet (SS.Applet Life Cycle Management).[16]
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 **physically overwrite the keys in randomised manner**[17] that meets the following: • **none**[18] Note: Cryptographic key destruction SFR is specified according to [PST].

[14] [assignment: list of cryptographic keys]
[15] [selection: no longer needed, [assignment: other circumstances]]
[16] [assignment: other circumstances]
[17] [assignment: *cryptographic key destruction method*]
[18] [assignment:*list of standards*]

*6.1.3.5 **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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_COP.1.1 / ECC	The TSF shall perform digital signature creation[19] in accordance with a specified cryptographic algorithm **ECDSA[20]** that meet the following: **ISO/IEC 14888-3, ANSI X9.62 and FIPS 186-5 [21].** The TSF supports cryptographic key sizes **256, 320, 384, 512, 521 bits[22]** over prime curves P-256, P-384, P-521, as defined in NIST Special Publication 800-186 [SP800-186][23] and Brainpool Standard Curves brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1 and brainpoolP512t1 defined in [RFC 5639].
FCS_COP.1.1 / ECDH	The TSF shall perform **key agreement**[24] operation in accordance with a specified cryptographic algorithm **ECDH**, that meet the following: **[SP800-56A][25]**. The TSF supports cryptographic key sizes **256, 320, 384, 512, 521 bits[26]** over prime curves P-256, P-384, P-521, as defined in NIST Special Publication 800-186 **[SP800-186][27]** and Brainpool Standard Curves brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1 and brainpoolP512t1 defined in [RFC 5639].

[19] [assignment: list of cryptographic operations]
[20] [assignment: cryptographic algorithm]
[21] [assignment: *list of standards*]
[22] [assignment: *cryptographic key sizes*]
[23] [assignment: *list of standards*]
[24] [assignment: *list of cryptographic operations*]
[25] [assignment: list of standards]
[26] [assignment: *cryptographic key sizes*]
[27] [assignment: *list of standards*]

*6.1.3.6 **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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_COP.1.1	The TSF shall perform digital signature creation[28] in accordance with a specified cryptographic algorithm **RSA[29] and RSA with PKCS#1 padding[30]** and cryptographic key sizes **RSA 3008 to 4096 bit[31]** that meet the following: • **[PKCS#1]**[32]
FCS_COP.1.1 / Decipher	The TSF shall perform decipher operation with a specified cryptographic algorithm **RSA[33] and RSA with PKCS#1 padding[34]** and cryptographic key sizes **RSA 3008 to 4096 bit[35]** that meet the following: • **[PKCS#1]**[36]
Note:	For RSA with PKCS#1 padding, both RSASSA-PKCS1-v_1_5 and RSASSA-PSS signature schemes specified in [PKCS#1] are supported for digital signature. Both specified schemes RSAES_PKCS1_v1_5 and RSAES-OAEP are supported for decipher-operations.

[28] [assignment: list of cryptographic operations]
[29] [assignment: *cryptographic algorithm*]
[30] [assignment: *cryptographic operation*]
[31] [assignment: *cryptographic key sizes*]
[32] [assignment: *list of standards*]
[33] [assignment: *cryptographic algorithm*]
[34] [assignment: *cryptographic operation*]
[35] [assignment: *cryptographic key sizes*]
[36] [assignment: *list of standards*]

*6.1.3.7 **FCS_COP.1 / AES** 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, or FCS_CKM.5 Cryptographic key derivation] FCS_CKM.3 Cryptographic key access FCS_CKM.6 Timing and event of cryptographic key destruction
FCS_COP.1.1 / AES	The TSF shall perform **data encryption and decryption** with a specified cryptographic algorithm **AES**[37] and cryptographic key sizes **AES 128, 192 and 256 bit**[38] that meet the following: • **[FIPS197], [SP 800-38A]**.[39] The TSF shall perform the following variations of the AES algorithms: **AES ECB, AES CBC, AES ECB with PKCS#7 padding, AES CBC with PKCS#7**[40] padding.

[37] [assignment: *cryptographic algorithm*]
[38] [assignment: *cryptographic key sizes*]
[39] [assignment: *list of standards*]
[40] [refinement: Included in [RFC 5652] list of standards]

6.1.4 User data protection (FDP)

6.1.4.1 General

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**	**PP reference**
S.User	Role	R.Admin, R.Sigy	[PP2] and [PP3]
S.User	SCD/SVD Management	authorised, not authorised	[PP2] and [PP3]
SCD	SCD Operational	no, yes	[PP2] and [PP3]
SCD	SCD identifier	arbitrary value	[PP2]
SVD	(This ST does not define security attributes for SVD)	(This ST does not define security attributes for SVD)	[PP2]

6.1.4.2 ***FDP_ACC.1/SCD/SVD_Generation*** *Subset access control [PP2]*

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[41] on:
1) subjects: S.User,
2) objects: SCD, SVD,
3) operations: generation of SCD/SVD pair[42].

6.1.4.3 ***FDP_ACF.1/SCD/SVD_Generation*** *Security attribute based access control [PP2]*

Hierarchical to: No other components.

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

FDP_ACF.1.1/ The TSF shall enforce the SCD/SVD Generation SFP1[43] to objects

[41] [assignment: access control SFP]
[42] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[43] [assignment: access control SFP]

SCD/SVD_Generation	based on the following: the user S.User is associated with the security attribute "SCD/SVD Management"[44].
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[45].
FDP_ACF.1.3/ SCD/SVD_Generation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[46].
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[47].

*6.1.4.4 **FDP_ACC.1/SVD_Transfer** Subset access control [PP2]*

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[48] on: 1) subjects: S.User; 2) objects: SVD; 3) operations: export[49].

*6.1.4.5 **FDP_ACF.1/SVD_Transfer** Security attribute based access control [PP2]*

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

[44] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]
[45] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[46] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[47] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[48] [assignment: access control SFP]
[49] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

FDP_ACF.1.1/ SVD_Transfer	The TSF shall enforce the SVD Transfer SFP[50] to objects based on the following: 1) the S.User is associated with the security attribute Role; 2) the SVD[51].
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[52].
FDP_ACF.1.3/ SVD_Transfer	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[53].
FDP_ACF.1.4/ SVD_Transfer	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: none[54].

*6.1.4.6 **FDP_ACC.1/Signature_Creation** Subset access control [PP2] and [PP3]*

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[55] on: 1) subjects: S.User; 2) objects: DTBS/R, SCD; 3) operations: signature creation[56].
Note:	This SFR is also applied to security objectives which are not defined in the PPs. In this case, the TSF shall enforce this access control SFP on 1) subjects: S.User; 2) objects: SCD, 3) operations: key agreement, data encipherment, data decipherment, key wrapping and key unwrapping.

*6.1.4.7 **FDP_ACF.1/Signature creation** Security attribute based access control [PP2] and [PP3]*

[50] [assignment: access control SFP]
[51] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]
[52] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[53] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[54] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[55] [assignment: access control SFP]
[56] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]

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[57] 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"[58].
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"[59].
FDP_ACF.1.3/ Signature_Creation	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[60].
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"[61].
Note:	This SFR is also applied to the cryptographic operations which are related to OT.Crypto_Op_Auth and not defined in the PPs. In this case, "signature creation" can be replaced with any of the operations.

*6.1.4.8 **FDP_RIP.1** Subset residual information protection [PP2] and [PP3]*

Hierarchical to:	No other components.
Dependencies:	No dependencies.

[57] [assignment: access control SFP]
[58] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFP-relevant security attributes, or named groups of SFP-relevant security attributes]
[59] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[60] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[61] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]

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[62] the following objects: SCD[63].

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".

*6.1.4.9 **FDP_SDI.2/Persistent** Stored data integrity monitoring and action [PP2] and [PP3]*

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[64] on all objects, based on the following attributes: integrity checked stored data[65].
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[66].

*6.1.4.10 **FDP_SDI.2/DTBS** Stored data integrity monitoring and action [PP2] and [PP3]*

Hierarchical to:	FDP_SDI.1 Stored data integrity monitoring.
Dependencies:	No dependencies.

[62] [selection: allocation of the resource to, deallocation of the resource from]
[63] [assignment: list of objects]
[64] [assignment: integrity errors]
[65] [assignment: user data attributes]
[66] [assignment: action to be taken]

FDP_SDI.2.1/DTBS	The TSF shall monitor user data stored in containers controlled by the TSF for integrity error[67] on all objects, based on the following attributes: integrity checked stored DTBS[68].
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[69].

6.1.4.11 FDP_ACC.1/SCD_Import Subset access control [PP3]

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[70] on (1) subjects: S.User, (2) objects: SCD, (3) operations: import of SCD[71].

6.1.4.12 FDP_ACF.1/SCD_Import Security attribute based access control [PP3]

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[72] to objects based on the following: the S.User is associated with the security attribute "SCD/SVD Management"[73].
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:

[67] [assignment: integrity errors]
[68] [assignment: user data attributes]
[69] [assignment: action to be taken]
[70] [assignment: access control SFP]
[71] [assignment: list of subjects, objects, and operations among subjects and objects covered by the SFP]
[72] [assignment: access control SFP]
[73] [assignment: list of subjects and objects controlled under the indicated SFP, and for each, the SFPrelevant security attributes, or named groups of SFP-relevant security attributes]

	S.User with the security attribute "SCD/SVD Management" set to "authorised" is allowed to import SCD[74].
FDP_ACF.1.3/ SCD_Import	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: none[75].
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[76].

6.1.4.13 FDP_ITC.1/SCD Import of user data without security attributes [PP3]

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[77] 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**.[78]

6.1.4.14 FDP_UCT.1/SCD Basic data exchange confidentiality [PP3]

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

[74] [assignment: rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects]
[75] [assignment: rules, based on security attributes, that explicitly authorise access of subjects to objects]
[76] [assignment: rules, based on security attributes, that explicitly deny access of subjects to objects]
[77] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[78] [assignment: *additional importation control rules*]

	FDP_IFC.1 Subset information flow control]
FDP_UCT.1.1/SCD	The TSF shall enforce the SCD Import SFP[79] to receive[80] ~~user data~~ **SCD** in a manner protected from unauthorised disclosure.

6.1.5 Identification and authentication (FIA)

*6.1.5.1 **FIA_UID.1** Timing of identification [PP2] and [PP3]*

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) **performing file management operations (SS.File Management) which are always allowed by file security attributes.** 3) **establishing a secure channel between CGA or other application and the TOE.** [81] 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.

*6.1.5.2 **FIA_UAU.1** Timing of authentication [PP2] and [PP3]*

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification.
FIA_UAU.1.1	The TSF shall allow:

[79] [assignment: access control SFP(s) and/or information flow control SFP(s)]
[80] [selection: transmit, receive]
[81] [assignment: *list of TSF-mediated actions*]

1) self-test according to FPT_TST.1;

2) identification of the user by means of TSF required by FIA_UID.1;

3) **performing file management operations (SS.File Management) which are always allowed by file security attributes.**

4) **establishing a secure channel between CGA or other application and the TOE.** [82]

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.

*6.1.5.3 **FIA_AFL.1** Authentication failure handling [PP2] and [PP3]*

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[83] **within the range from 1 to 14**[84] unsuccesful authentication attempts occur related to consecutive failed authentication attempts[85].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met[86], the TSF shall block RAD[87].

[82] [assignment: *list of TSF mediated actions*]
[83] [assignment: *number of allowed authentication attempts*]
[84] [assignment: *configurable range of authentication attempts*]
[85] [assignment: list of authentication events]
[86] [selection: met, surpassed]
[87] [assignment: list of actions]

6.1.6 Security management (FMT)

6.1.6.1 FMT_SMR.1 Security roles [PP2] and [PP3]

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[88].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.

6.1.6.2 FMT_SMF.1 Security management functions [PP2] and [PP3]

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; only in [PP2] 5) **Unblocking a blocked RAD**[89].

Note that the SFRs taken from [PP2] and [PP3] have been merged.

[88] [assignment: the authorised identified roles]
[89] [assignment: *list of other security management functions to be provided by the TSF*]

6.1.6.3 FMT_MOF.1 Management of security functions behaviour [PP2] and [PP3]

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[90] the functions signature creation function[91] to R.Sigy[92].

6.1.6.4 FMT_MSA.1/Admin Management of security attributes [PP2] and [PP3]

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 [PP2] and [PP3]	The TSF shall enforce the SCD/SVD Generation SFP and SCD Import SFP[93] to restrict the ability to modify, **none**[94] the security attributes SCD/SVD management[95] to R.Admin[96].

Note that the SFRs taken from [PP2] and [PP3] have been merged.

6.1.6.5 FMT_MSA.1/Signatory Management of security attributes [PP2] and [PP3]

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

[90] [selection: determine the behaviour of, disable, enable, modify the behaviour of]
[91] [assignment: list of functions]
[92] [assignment: the authorised identified roles]
[93] [assignment: access control SFP(s), information flow control SFP(s)]
[94] [selection: change, default, query, modify, delete, [assignment: *other operations*]]
[95] [assignment: list of security attributes]
[96] [assignment: the authorised identified roles]

FMT_MSA.1.1/Signatory	The TSF shall enforce the Signature Creation SFP[97] to restrict the ability to modify[98] the security attributes SCD operational[99] to R.Sigy[100].

6.1.6.6 FMT_MSA.2 Secure security attributes [PP2] and [PP3]

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[101]).

6.1.6.7 FMT_MSA.3 Static attribute initialization [PP2] and [PP3]

Hierarchical to:	No other components.
Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles
FMT_MSA.3.1 [PP2]	The TSF shall enforce the SCD/SVD Generation SFP, SVD Transfer SFP and Signature Creation SFP[102] to provide restrictive[103] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.1 [PP3]	The TSF shall enforce the SCD Import SFP and Signature Creation SFP[104] to provide restrictive[105] default values for security attributes that are used to enforce the SFP.

[97] [assignment: access control SFP(s), information flow control SFP(s)]
[98] [selection: change_default, query, modify, delete, [assignment: other operations]]
[99] [assignment: list of security attributes]
[100] [assignment: the authorised identified roles]
[101] [selection: *list of security attributes*]
[102] [assignment: access control SFP, information flow control SFP]
[103] [selection, choose one of: restrictive, permissive, [assignment: other property]]
[104] [assignment: *access control SFP, information flow control SFP*]
[105] [selection, choose one of: *restrictive, permissive, [assignment: other property]*]

FMT_MSA.3.2 [PP2] and [PP3]	The TSF shall allow the R.Admin[106] to specify alternative initial values to override the default values when an object or information is created.

Note that the SFRs taken from [PP2] and [PP3] have been merged.

6.1.6.8 FMT_MSA.4 Security attribute value inheritance [PP2] and [PP3]

Hierarchical to:	No other components.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]
FMT_MSA.4.1 [PP2]	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.[107]
FMT_MSA.4.1 [PP3]	The TSF shall use the following rules to set the value of security attributes: 1) 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. 2) 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.[108]

Note that the SFRs taken from [PP2] and [PP3] have been merged.

6.1.6.9 FMT_MTD.1/Admin Management of TSF data [PP2] and [PP3]

[106] [assignment: the authorised identified roles]
[107] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[108] [assignment: *rules for setting the values of security attributes*]

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[109] the RAD[110] to R.Admin[111].

6.1.6.10 FMT_MTD.1/Signatory Management of TSF data [PP2] and [PP3]

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**[112] the RAD[113] to R.Sigy[114].

6.1.7 Protection of the TSF (FPT)

6.1.7.1 FPT_EMS.1 Emanation of TSF and User data

Hierarchical to:	No other components.
Dependencies:	No dependencies.
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 9:

Table 9 - FPT_EMS.1.1 Table

ID	Emissions	Attack surface	TSF data	User data

[109] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[110] [assignment: *list of TSF data*]
[111] [assignment: *the authorised identified roles*]
[112] [selection: *change_default, query, modify, delete, clear, [assignment: other operations]*]
[113] [assignment: *list of TSF data*]
[114] [assignment: the *authorised identified roles*]

1	variations in power consumption or timing during command execution[115]	Electrical contacts or Radio Frequency (RF) field. [116]	Cryptographic data used in runtime cryptographic computations. [117]	RAD, SCD[118].

Note: In [PP2] and [PP3] FPT_EMS.1 is defined as an extended component. Due to adoption of CC:2022, this SFR is defined in the ST in accordance with section 15.2 of the CC:2022 Part 2 and not as an extended component.

6.1.7.2 FPT_FLS.1 Failure with preservation of secure state [PP2] and [PP3]

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) **Failed authentication or insufficient authentication state, failed command parameter validation, failure of an internal consistency check, types of failures defined in [PST]/FPT_FLS.1.**[119]

6.1.7.3 FPT_PHP.1 Passive detection of physical attack [PP2] and [PP3]

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.

[115] [assignment: types of emissions]
[116] [assignment: list of types of attack surface]
[117] [assignment: list of types of TSF data]
[118] [assignment: list of types of user data]
[119] [assignment: *list of types of failures in 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.

6.1.7.4 FPT_PHP.3 Resistance to physical attack [PP2] and [PP3]

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_PHP.3.1	The TSF shall resist **physical manipulation and physical probing**[120] to the **TSF**[121] by responding automatically such that the SFRs are always enforced.

6.1.7.5 FPT_TST.1 TSF testing [PP2] and [PP3]

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_TST.1.1	The TSF shall run a suite of self tests at the request of the authorised user, at the conditions: **the TOE is in creation state or in operational state** to demonstrate the correct operation of the TSF[122].
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of TSF data[123].
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of TSF[124].

[120] [assignment: *physical tampering scenarios*]
[121] [assignment*: list of TSF devices/elements*]
[122] [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]]
[123] [selection: [assignment: parts of TSF data], TSF data]
[124] [selection: [assignment: parts of TSF], TSF]

6.1.7.6 FTP_ITC.1/SCD Inter-TSF trusted channel [PP3]

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[125] 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**[126].
Note:	RAD and VAD can be optionally transferred via trusted channel, but this is not required.

[125] [selection: the TSF, another trusted IT product]
[126] [assignment: *list of functions for which a trusted channel is required*]

6.2 Security Assurance Requirements

Table 10: Assurance Requirements: EAL4 augmented with AVA_VAN.5

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Architectural Design with domain separation and nonbypassability
	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

6.3.1 Security Assurance Requirements Rationale

The targeted assurance level for evaluation is EAL4 augmented. The assurance requirements where chosen based on the selected PPs, where the required assurance components have been listed. EAL4 allows a developer to attain a reasonably high assurance level without the need for highly specialised 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. The TOE described is just such a product. MyEID is an existing product, which previous versions mostly fulfil requirements of EAL4 augmented. The features required to fulfil rest of the requirements have been developed to the TOE. EAL4 has been considered to be the right choice based on commercial needs, security requirements of users of the TOE and amount of work needed to accomplish this level.

Augmentation results from the selection of:

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.

This ST includes security objectives and associated SFRs from outside the selected PPs. The requirements are very similar in nature to core requirements of the PPs, and TSF associated with them is technically very similar to functionality directly associated with the PPs. Therefore, the same assurance components have been considered to be appropriate to fulfil EAL4 augmented level requirements for these objectives.

6.3.2 Security Requirement Coverage

The following table provides mapping of TOE security objectives to related functional requirements. The objectives and SFRs marked with [PP2] or [PP3] are taken from this specific PP. The objectives and SFRs with no marking and white background are included in both PPs. The objectives marked with grey background are not included in the PPs. They are related to TOEs functionality not covered by the PPs.

Table 11: Mapping of functional requirements to security objectives for the TOE

TOE security objectives / Functional requirements	OT.Lifecycle_Security	OT.SCD/SVD_Auth_Gen **[PP2]**	OT.SCD_Auth_Imp **[PP3]**	OT.SCD_Unique **[PP2]**	OT.SCD_SVD_Corresp **[PP2]**	OT.SCD_Secrecy	OT.Sig_Secure	OT.Sigy_SigF	OT.DTBS_Integrity_TOE	OT.EMSEC_Design	OT.Tamper_ID	OT.Tamper_Resistance	OT.Key_Agreement_Security	OT.Secure_Encipherment	OT.Crypto_Op_Auth
FCS_CKM.1 **[PP2]**	X	X		X	X	X				X					
FCS_CKM.3	X					X									
FCS_CKM.6	X					X									
FCS_COP.1	X					X	X	X	X	X			X	X	
FDP_ACC.1/SCD/SVD_Generation **[PP2]**	X	X													
FDP_ACC.1/SCD_Import **[PP3]**	X		X												
FDP_ACC.1/Signature_Creation	X							X							X
FDP_ACC.1/SVD_Transfer **[PP2]**	X														
FDP_AFC.1/SCD/SVD_Generation **[PP2]**	X	X													
FDP_AFC.1/SCD_Import **[PP3]**	X		X												
FDP_AFC.1/Signature_Creation	X							X							
FDP_AFC.1/SVD_Transfer **[PP2]**	X														
FDP_ITC.1/SCD **[PP3]**	X														
FDP_RIP.1						X							X		
FDP_SDI.2/DTBS	X							X	X						
FDP_SDI.2/Persistent	X				X	X	X								
FDP_UCT.1/SCD **[PP3]**	X		X			X									
FIA_AFL.1								X							

FIA_UAU.1		X	X					X					X	X	X
FIA_UID.1		X	X					X					X	X	X
FMT_MOF.1	X							X							X
FMT_MSA.1/Admin	X	X													
FMT_MSA.1/Signatory	X							X							X
FMT_MSA.2	X	X	X					X							X
FMT_MSA.3	X	X	X					X							X
FMT_MSA.4	X	X						X							
FMT_MTD.1/Admin	X							X							
FMT_MTD.1/Signatory	X							X							
FMT_SMF.1	X				X			X							
FMT_SMR.1	X							X							
FPT_EMS.1						X				X					
FPT_FLS.1						X		X							X
FPT_PHP.1											X				
FPT_PHP.3						X						X			
FPT_TST.1	X					X		X							
FTP_ITC.1/SCD **[PP3]**	X					X									

6.3.3 SFR Dependency Rationale

Sufficiency and satisfaction of dependencies of security requirements are as defined in [PP2] and [PP3] section 9.3.3, tables 5 and 6 (same for both PPs), with a few exceptions resulting from transition from CC V3.1 R5 to CC:2022, taking [CC2022_EI] in account. The dependencies have been updated as follows:

Functional requirement	**Dependencies**	**Satisfied by**
FCS_CKM.1 / RSA	[FCS_CKM.2 or FCS_CKM.5 Or FCS_COP.1] [FCS_RBG.1 or FCS_RNG.1] FCS_CKM.6	FCS_COP.1 / RSA FCS_RNG.1 FCS_CKM.6
FCS_CKM.1 / ECC	[FCS_CKM.2 or FCS_CKM.5 Or FCS_COP.1] [FCS_RBG.1 or FCS_RNG.1] FCS_CKM.6	FCS_COP.1 / ECC FCS_RNG.1 FCS_CKM.6
FCS_CKM.3	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5]	FDP_ITC.1/SCD
FCS_CKM.6	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1.* FDP_ITC.1/SCD
FCS_COP.1 / RSA	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.6	FDP_ITC.1/SCD FCS_CKM.1/RSA FCS_CKM.6
FCS_COP.1 / ECC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.6	FDP_ITC.1/SCD FCS_CKM.1/ECC FCS_CKM.6
FCS_COP.1 / AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1 or FCS_CKM.5] FCS_CKM.3 FCS_CKM.6	FDP_ITC.1/SCD FCS_CKM.6

FCS_CKM.4 has been deprecated and replaced by FCK_CKM.6. FCS_CKM.3 is related to the key wrapping / unwrapping feature, which is out-of-scope of [PP2] and [PP3]

6.3.4 TOE Security Functional Requirements Sufficiency

[PP2] combined with [PP3]
OT.Lifecycle_Security (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 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_ICT.1/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 secure SCD usage is ensured cryptographically according to FCS_COP.1. The SCD usage is ensured/controlled by access control FDP_ACC.1/Signature_Creation, FDP_AFC.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. The FMT_SMF.1 and FMT_SMR.1 defines security management rules and functions. The test functions FPT_TST.1 provides failure detection throughout the lifecycle. The SFR FCS_CKM.6 ensures a secure SCD destruction.

FDP_SDI.2/Persistent ensures that the TOE detects integrity errors of integrity checked stored data and informs the user S.Sigy about it and therefore contributes to flaw detection during operation. The TOE relies on platform's features associated with platform SFR_FDP_SDI.2 to fulfil this requirement.

Platform SFRs support fulfilling the SFRs related to this objective as described in section 1.3.1 - Platform SFRs Used by This Composite ST.

[PP2]**OT.SCD/SVD_Auth_Gen** (Authorised SCD/SVD generation) 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.

[PP3]
OT.SCD_Auth_Imp (Authorised SCD import) 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.

[PP2]
OT.SCD_Unique (Uniqueness of the signature creation data) implements the requirement of practically unique SCD as laid down in Annex III, paragraph 1(a), which is provided by the cryptographic algorithms specified by FCS_CKM.1.

[PP2]
OT.SCD_SVD_Corresp (Correspondence between SVD and SCD) 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.

[PP2] combined with [PP3]
OT.SCD_Secrecy (Secrecy of signature creation data) 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 and SFR. FDP_UCT.1/SCD and FTP_ICT.1/SCD ensures the confidentiality for SCD import.

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).
SFR FPT_EMS.1 and FPT_PHP.3 require additional security features of the TOE to ensure the confidentiality of the SCD.

[PP2] and [PP3]
OT.Sig_Secure (Cryptographic security of the electronic signature) 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.

[PP2] combined with [PP3]
OT.Sigy_SigF (Signature creation function for the legitimate signatory only) 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.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_MOF.1 ensures that only the signatory can enable/disable the signature creation function.
FMT_MSA.1/Signatory restricts the ability to modify the security attributes SCD operational to the signatory.

Furthermore, the security functionality specified by FDP_RIP.1 will ensure that no attacker can get hold of the SCD (to create signatures outside the TOE) once SCD have been deleted by the legitimate signatory.

[PP2] and [PP3]
OT.DTBS_Integrity_TOE (DTBS/R integrity inside the 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.
The verification that the DTBS/R has not been altered by the TOE is provided by integrity functions specified by FDP_SDI.2/DTBS.

[PP2] and [PP3]
OT.EMSEC_Design (Provide physical emanations security) covers that no intelligible information is emanated. This is provided by FPT_EMS.1.1.

[PP2] and [PP3]
OT.Tamper_ID (Tamper detection) is provided by FPT_PHP.1 by the means of passive detection of physical attacks.

[PP2] and [PP3]
OT.Tamper_Resistance (Tamper resistance) is provided by FPT_PHP.3 to resist physical attacks.

OT.Key_Agreement_Security is provided by FCS_COP.1.1 / ECDH, which defines the cryptographic algorithm and allowed parameters used for key agreement and ensures cryptographic robustness of the implementation. FIA_UAU.1 and FIA_UID.1 ensure that the key agreement function cannot be invoked before the user is identified and authenticated. FDP_RIP.1 prevents misuse of any resources containing the SCD after de-allocation (e.g. using it for computing the shared secret for key agreement).

OT.Secure_Encipherment is provided by FCS_COP.1 / AES, which defines the cryptographic algorithm and allowed parameters used for data encipherment. FIA_UAU.1 and FIA_UID.1 ensure that the encipherment function cannot be invoked before the user is identified and authenticated.

OT.Crypto_Op_Auth is provided by FIA_UAU.1 and FIA_UID.1, which ensure that cryptographic function (key agreement, data encipherment, data decipherment, key wrapping and key unwrapping) can be invoked before the user is identified and authenticated. FDP_ACC.1/Signature_Creation provides access control based security on attributes. In context of the cryptographic operations related to this OT, this SFR is applied for the operations in similar way as for the Signature Creation operation: It ensures that access for using the key (SCD) associated with the operation is granted only for authenticated user. The security attributes are managed according to the SFRs FMT_MSA.1/Signatory, FMT_MSA.2 and FMT_MSA.3. FPT_FLS.1 guarantees a secure state in case integrity of the TOE is violated and thus assures that the specified security functions are operational and cannot be bypassed.

6.3.5 Security Requirements – Internal Consistency

The following part of the security requirements rationale shows that the set of security requirements for the TOE consisting of the security functional requirements (SFRs) and the security assurance requirements (SARs) together forms an internally consistent whole.

The analysis of the TOE´s security requirements with regard to their mutual supportiveness and internal consistency demonstrates:

> The dependency analysis in section 6.3.3 ‘SFR Dependency Rationale‘ for the security functional requirements shows that the basis for internal consistency between all defined functional requirements is satisfied. All dependencies between the chosen functional components are analysed and non-satisfied dependencies are appropriately explained.
>
> All subjects and objects addressed by more than one SFR in sec. 6.1 are also treated in a consistent way: the SFRs impacting them do not require any contradictory property and behaviour of these ‘shared’ items.
>
> The assurance package EAL4 is a pre-defined set of internally consistent assurance requirements. The dependency analysis for the sensitive assurance components in section 6.3.1 ‘Security Assurance Requirements Rationale’ shows that the assurance requirements are internally consistent as all (additional) dependencies are satisfied and no inconsistency appears.

Inconsistency between functional and assurance requirements could only arise, if there are functional-assurance dependencies being not met: an opportunity shown not to arise in sections 6.3.3 ‘SFR Dependency Rationale‘ and 6.3.1 ‘Security Assurance Requirements Rationale’. Furthermore, as also discussed in section 6.3.1 ‘Security Assurance Requirements

Rationale', the chosen assurance components are adequate for the functionality of the TOE. So, there are no inconsistencies between the goals of these two groups of security requirements.

7 TOE Summary Specifications

The TOE provides multiple security services (SS) and security features (SF) which will be further described in the following subsections. The core functions, SS and SF, of the TOE are listed below and described in detail. The same security services and security features can be used vie the MyEID command interface and the PIV command interface. MyEID command interface supports all services and features, while PIV command interface supports those included in the PIV specification. The descriptions include explanation, how the most relevant SFRs are fulfilled by the service or feature. The full mapping between each SS and SF, and related SFRs is provided in 7.3

7.1 Security Services

7.1.1 SS.Signature Creation

The TOE provides a service to create signatures using RSA (FCS_COP.1/RSA) or ECC (FCS_COP.1/ECC) algorithms. For this it uses the cryptographic libraries provided by the platform. Signature creation is subject to access control and only available to authenticated users (FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation).

7.1.2 SS.User Authentication

The TOE authenticates users using authentication objects, which can be either an alphanumeric PIN code or a challenge/response PIN. The TOE verifies authentication data provided by user, a PIN or a response to a challenge, and opens specific access conditions upon successful verification. Security attribute based access conditions open rights for example to use a private key for signature creation. Each authentication object can be mapped to allow a specific operation. The challenge/response mechanism uses a secret key with AES algorithm to authenticate response to a random challenge that the TOE provides to the user.

7.1.3 SS.Data Decipherment

The TOE has capability to decipher data with a private key or with a symmetric secret key. User provides data that has been enciphered with the associated public key or with the identical secret key. Decipher-operation requires user authentication. The TOE uses platform's functionality to perform data decipherment. This security service fulfils FCS_COP.1/RSA and FCS.COP.1/AES. Access control is implemented similarly as in signature creation, by protecting access to use the private or secret key, as required by FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation.

7.1.4 SS.Data Encipherment

The TOE has capability to encipher data with a secret key using a symmetric encryption algorithm. The encipher-operation requires user authentication. The TOE uses platform's

functionality to perform data encipherment. This security service fulfils FCS.COP.1/AES Access control is implemented similarly as in signature creation, by protecting access to use the secret key, as required by FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation.

7.1.5 SS.Key Generation

The TOE has capability to generate RSA and ECC keys pairs. The TOE uses platform's functionality to perform key generation. User of TOE must be authenticated with key generation access right to the key file where the key is to be generated.

7.1.6 SS.Key Import

The TOE has capability to import an RSA or ECC key pair. User of TOE must be authenticated with key generation access right to the key file where the key is to be imported into. This security service fulfils FDP_UCT.1/SCD when a secure channel is used to import the SCD as instructed in the user guidance. Access to the key import function is controlled as required by FDP_ACC.1 and FDP_ACF.1/SCD_Import.

7.1.7 SS.Key Wrapping

The TOE has capability to use its data encipherment capability to encrypt symmetric keys stored on the card using another symmetric key, and to output the encrypted key material. The function is available for secret keys, only if it has been enabled when the key is created into the card. RSA or ECC keys cannot be wrapped. Key wrapping operation requires user authentication.

7.1.8 SS.Key Unwrapping

The TOE has capability to use its data decipherment feature to decipher encrypted key material and install the key into the TOE. The Key Unwrapping function can be used to securely transfer a private or secret key to the TOE over insecure environment. The key data does not leave the TOE during this operation and is not extractable in plain text later. Key unwrapping operation requires user authentication. This security service is another way to fulfil FDP_UCT.1/SCD and FTP_ITC.1.1/SCD, and allows transferring the SCD from another environment or over unsecure network. Access to the key unwrapping function is controlled as required by FDP_ACC.1 and FDP_ACF.1/SCD_Import. This feature can only be used to unwrap symmetric keys and SCD refers to symmetric keys in this context.

7.1.9 SS.Secure Key Storage

The TOE ensures safe storage of private keys. It has been designed so that generated or imported private keys cannot be exported from it. The TOE uses the platform's functionality to store private keys. The security service is associated with FPT_EMS.1, FPT_FLS.1, FPT_PHP.1 and FPT.PHP3 and the platform’s security services which are used to fulfil these SFRs.The TOE relies on the platform on protection against side-channel attacks and physical tampering, and the internal architecture of the TOE ensures that SCD cannot be retrieved using the command interface.

7.1.10 SS.Key Argeement

The TOE has capability to generate a shared secret using ECDH algorithm. In an ECDH operation, the other party provides his or her public key. The owner of the TOE uses the other party's public key, and the private key on the TOE, to generate the secret. The other party uses TOE owner's public key and his or her private key to do the same operation. The operation results into the same shared secret on both sides. Key agreement requires user authentication. The TOE uses platform's functionality to perform the ECDH operation. This security service complies with FCS_COP.1.1 / ECDH. Access to the key agreement function is protected according to FDP_ACC.1/Signature_Creation, FDP_ACF.1/Signature_Creation..

7.1.11 SS.File Management

The TOE provides functions to create, modify and delete files, which can contain cryptographic keys, certificates and other data. The files can be protected with configurable security attributes. Security attributes define, which operations require user authentication. This security service is associated with FMT_SMR.1, FDP_ACC.1 and FDP_ACF.1. User role based security attributes are defined for each file.

7.1.12 SS.Authentication Management

The TOE provides functions to create authentication objects e.g. PINs and to map them to security attributes of files and keys. With authentication objects, different access rights can be defined for users and administrators. This security service is related to SFRs FMT_SMR.1, FDP_ACC.1 and FDP_ACF.1. By authenticating to a role associated with an authentication object, user gains access to files associated with the role. Authentication management includes a secure, configurable mechanism to unblock a blocked authentication object.

7.1.13 SS.Applet Life Cycle Management

The TOE provides services to manage those states of applet life cycle, which are applicable after the TOE has been delivered from Aventra. Life cycle management includes switching from Creation State, where authentication objects can be created, to Operational State, and erasing all data from the TOE.

7.2 Security features

7.2.1 SF.Applet Hardening

Applet hardening is implemented by applying non-bypassability and self-protection principles in the applet's code design, and by relying on the platform's features in domain separation, self-protection (FPT_FLS.1), emanation security (FPT_EMS.1) and resistance to physical attacks (FPT_PHP.3). In the applet's design, hardening is achieved by enforcing access conditions in the same systematic way in all security services, by requiring all checks to be passed before access to use SCD is given, and by following the platform's user guidance. Furthermore, SCD is not exposed to the apple's memory space in crypto-operations, as they are performed using the platform's services.

7.2.2 SF.Platform Security Functionality

The TOE uses the platform's security functions and features to protect itself from unauthenticated access. The platform's security features protect the sensitive objects such as SCD and RAD on the TOE from attacks. The TOE relies on platform especially on physical protection, using its features to fulfil FPT_EMS.1 (FPT_EMSEC.1 in platform ST), FPT_PHP.1 and FPT_PHP.3 (same SFR in the platform ST). The platform's functionality is also used to ensure that FCS_CKM.1 and FCS_COP.1 are fulfilled properly, using platform's evaluated implementations of key generation, signature creation and other cryptographic algorithms. The TOE relies on platform's features to fulfil FDP_RIP.1 and FDP_SDI.2.

7.2.3 SF.Secure Messaging

The TOE provides a feature to establish an encrypted channel to transfer information between the TOE and the software communicating with the TOE. Secure Messaging is used to ensure confidentiality of VAD in user authentication, RAD in authentication management and confidentiality of SCD, when importing the SCD into the TOE. The TOE supports the key establishment protocol described in [PIV] for key agreement. The TOE uses the secure messaging protocol defined in ISO 7816-4 standard. This security feature fulfils SFRs FDP_UCT.1/SCD and FTP_ITC.1/SCD.

7.3 Summary of Specification Rationale

Table 12: SFRs mapped to Security Services and Features

	Security Services												Security Features		
Security Services and Features / SFRs	SS.Signature Creation	SS.User Authentication	SS.Data Decipherment	SS.Data Encipherment	SS.Key Generation	SS.Key Import	SS.Key Wrapping	SS.Key Unwrapping	SS.Secure Key Storage	SS.Key Agreement	SS.File Management	SS.Authentication Management	SS.Applet Life Cycle Management	SF.Applet Hardening	SF.Platform Security Functionality	SF.Secure Messaging
FCS_CKM.1 / ECC					X				X						X	
FCS_CKM.1 / RSA					X				X						X	
FCS_CKM.3							X									
FCS_CKM.6									X						X	
FCS_COP.1 / ECC	X									X					X	
FCS_COP.1 / RSA	X		X												X	
FCS_COP.1 / AES			X	X											X	
FDP_ACC.1/SCD/SVD_Generation **[PP2]**		X														
FDP_ACC.1/SVD_Transfer **[PP2]**		X														
FDP_ACC.1/SCD_Import **[PP3]**		X				X		X								
FDP_ACC.1/Signature_Creation	X	X														
FDP_ACF.1/SCD/SVD_Generation **[PP2]**		X			X											
FDP_ACF.1/SVD_Transfer **[PP2]**		X														
FDP_ACF.1/SCD_Import **[PP3]**		X				X		X								

FDP_ACF.1/Signature_Creation	X	X													
FDP_ITC.1/SCD [PP3]						X		X			X				
FDP_RIP.1									X		X				
FDP_SDI.2/Persistent														X	
FDP_SDI.2/DTBS														X	
FDP_UCT.1/SCD [PP3]						X		X							X
FIA_AFL.1		X												X	
FIA_UAU.1		X													
FIA_UID.1		X													
FMT_MOF.1	X	X													
FMT_MSA.1/Admin		X										X	X		
FMT_MSA.1/Signatory		X										X	X		
FMT_MSA.2												X			
FMT_MSA.3					X	X		X				X			
FMT_MSA.4		X			X	X		X							
FMT_MTD.1/Admin												X			
FMT_MTD.1/Signatory												X			
FMT_SMR.1												X			
FMT_SMF.1												X	X		
FPT_EMS.1														X	
FPT_FLS.1														X	X
FPT_PHP.1														X	
FPT_PHP.3														X	
FPT_TST.1															X

FTP_ITC.1/SCD **[PP3]**							X							X