Aventra MyEID PKI Smart Card

Reference manual

ANNEX I – Common Criteria EAL4+ Compliance
Ver. 3.0.8

Public

Aventra Ltd.
Kutomotie 16
00380 Helsinki
Finland

VAT number: FI8940682
www.aventra.fi
Tel. +358 9 4251 1251
sales@aventra.fi

Contents

Version history

Date	Version	Description
28.9.2022	0.1	Initial version
8.2.2024	3.0.0	Ready for evaluation
28.6.2024	3.0.1	Added explanation on how the requirements for the operational environment can be fulfilled.
15.10.2024	3.0.3	Changed document / product name to be consistent with other CC EAL4+ certification documentation.
3.12.2024	3.0.4	Mentioned that it is a requirement to configure a separate user and admin PIN. Internal review 16.12.2024 JS
6.2.2025	3.0.5	Changed document name and placement of version number, so in future versions this annex may have different version number than the main document. Internal review 7.2.2025 JS
14.3.2025	3.0.6	Updated 5.2.9, taking requirements of the Protection Profile 419211-3:2013 for SSCD with key import into account. Internal review 16.3.2025 JS
18.8.2025	3.0.7	Updated introduction, specified MyEID version, which this document applies to. Internal review 22.8.2025 JS
27.1.2025	3.0.8	Updated description of OE.SVD_Auth to be in line with ST 1.17 updates. Added 6.1, defined 3008 bits as the minimum allowed RSA key length, as required by SOGIS-ACM Internal review 12.2.2026, JS

1 Introduction

Aventra MyEID PKI Card Smart card version 5.0.0 is being evaluated as Common Criteria EAL4+ compliant. Protection Profiles for Secure Signature Creation Device, parts 1-3 are used in the evaluation. The protection profiles contain some requirements, which require setting up and using MyEID PKI Card in a specific way. The terminology used in the Protection Profiles and other Common Criteria is partly different than the terminology used in MyEID PKI Smart Card Reference Manual. The purpose of this document is to provide instructions on how to set up and use MyEID version 5.0.0 in fully EAL4+ compliant way and provide mapping between the terminologies.

2 References

The most relevant specifications and standards are:

- ISO/IEC 7816-4
- ISO/IEC 7816-8
- ISO/IEC 7816-9
- ISO/IEC 7816-15
- JavaCard 2.1.1, MyEID3: 2.2.1, MyEID5: 3.0.5
- GlobalPlatform 2.0.1 (Open Platform), MyEID3: GlobalPlatform 2.1.1, MyEID5: GlobalPlatform 2.3.1
- FINEID S1 and S4 documentation
- PIV/CIV
- [CMP] Certificate Management Protocol (CMP): https://datatracker.ietf.org/doc/html/rfc4210
- [MS-WCCE] Windows Client Certificate Enrollment Protocol: https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-wcce/446a0fca-7f27-4436-965d-191635518466
- [SOGIS-ACM] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.3.pdf

3 Abbreviations

AC	Access Condition
AID	Application Identifier
APDU	Application Protocol Data Unit
ASN.1	Abstract Syntax Notation One
CRDO	Control Reference Data Object
CIV	Commercial Identity Verification
CLA	Class Byte
C/R	Challenge/Response
DF	Dedicated File
EF	Elementary File
Key EF	Elementary File for cryptographic keys
FCI	File Control Information
FID	File Identifier
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
RA	Registration Authority

3.1 Common Criteria specific

SFR	Security Functional Requirement
SCD	Signature Creation Data
DTBS	Data To Be Signed
CGA	Certificate Generation Application

CSP Certification Service Provider

4 Terminology mapping

Terminology used in Common Criteria Protection Profiles for Secure Signature Creation Devices (SSCD) differs in some parts from the terminology used in MyEID documentation and user guidance. The following table maps abbreviations and terms used in the PPs to terminology used in MyEID documentation.

Table 1 - Regular usage related commands of the MyEID applet.

Common Criteria	MyEID documentation	Explanation
SCD Signature Creation Data	Private key	Signature Creation Data means private keys in context of smart cards.
DTBS Data To Be Signed	-	
DTBS / R Data to be signed or its unique representation	Hash	Hash of the data to be signed.
SVD Signature Verification Data	Public key	
RAD Reference Authentication Data	PIN, authentication object	RAD refers to the value user provides to authenticate to the card. An authentication object in MyEID card contains the RAD and associated information, such as PIN metadata (name, id, etc.), maximum failed attempts and counter of failed attempts.
Signatory	End user	The owner of the private key used for creating digital signatures
Admin	Administrator / SO	Security Officer (SO) in PKCS#15 / PKCS#11 terminology.
CSP, CGA	CA	The term Certification Authority refers to the terms CSP and CGA together
SSCD provisioning service	Registration Authority / RA	The service, which requests certificates from a CA, personalises the TOE for the Signatory and deliver the TOE to the Signatory.

Installation	Initialisation	In CC documentation "installation" is defined as "the procedures that the user has to perform normally only once after receipt and acceptance of the TOE to progress it to the secure configuration as described in the ST including the embedding of the TOE in its operational environment." MyEID applet is loaded into the JavaCard platform only in Aventra's production. To avoid confusing applet loading with the initialization done by the customers, term "Initialisation" is preferred in MyEID documentation. Initialisation consists of issuing the PUT DATA: INITIALISE APPLET command, creating the file structure, initialising PIN codes, activating the applet, generating or importing keys and loading certificates.

5 Requirements for the operational environment

This section contains description how the security objectives for the operational environment defined in the Security Target of MyEID are met and what must be taken into account to fulfil them.

5.1 Overview

The following principles shall be followed to ensure that the defined security objectives are fulfilled:

- Ensure that the applications and middleware software are trusted.
- Ensure that normal security related best-practices, like having virus protection and a firewall, and a regularly updated operating system, are followed.
- Use either a pinpad-reader or secure messaging to protect the PIN code (VAD).
- Use secure channel and ensure proper key management for the whole life cycle of the SCD, in case you import SCD to the TOE.
- Ensure that the environment where PIN codes (RAD/VAD) are created and loaded to the card and the environment where keys are imported to the card is secure. It is recommended to perform applet initialization and the related tasks like creation of the file system and PIN codes in an offline-environment or in an environment where internet access is restricted using hardware firewalls so that there is no direct access to internet.
- Use challenge/response PINs with AES algorithm. Do not use Triple-DES challenge/response PINs.

- A Security Specialist with knowledge of IT security and PKI reviews the system as a whole and verifies that the requirements are fulfilled, and correct configuration options are selected.

There are no specific hardware requirements. Any ISO 7816 1-4 compliant smart card reader can be used.

5.2 Requirements

In this section, each requirement is considered separately.

5.2.1 OE.SVD_Auth Authenticity of the SVD [PP2 / PP3]

A Security Specialist shall ensure that the selected CA system and connection protocol together ensure the integrity and authenticity of the SVD sent to the CGA of the CSP. This is usually done by signing the certificate request with the private key (SCD) of the signatory. By verifying the signature, the CGA ensures that the SVD corresponds with the SCD. An RA certificate is usually required to verify that the certificate request originates from a trusted source. It is responsibility of the RA to verify the identity of the End user the certificate is issued for and to ensure that the SCD is stored in the SSCD (MyEID card).

These requirements are addressed in commonly used CA systems and certificate request protocols in slightly different ways. The requirements are taken into account in for example [CMP] protocol and Windows Client Certificate Enrolment Protocol [MS WCCE].

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

a) Operators of the RA which requests certificates for the signatory from a CA shall be trained to verify the identity of the signatory. It is RA's responsibility to ensure that the TOE is handed over to the signatory, whose name is in the qualified certificate associated with the SCD.

b) By configuring the USE security attribute of the Key EF which contains the SCD is associated with the personal PIN code (RAD) of the signatory, and ensuring, with the methods described in section 15.3 of the reference manual, that nobody else gains access to the PIN code, it is ensured that the SCD stored in the TOE is under sole control of the signatory.

c) The certificate, which contains the name of the signatory and is associated with the SCD is signed by the CSP. The issuer's (CSPs) certificate shall be installed either to the TOE or into the IT infrastructure (for example Windows domain), where the TOE is used. It is a responsibility of a Security Specialist to ensure that authenticity of the issuer's signature is verified and that the chain of signatures up to the root CA certificate is verified.

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

The personnel operating the RA (SSCD provisioning service) shall be trained to verify identity of the Signatory and to follow necessary security measures to ensure authenticity of the TOE.

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

To fulfil this requirement, either a smart card reader equipped with a pin pad shall be used, or VAD shall be transmitted using a secure channel. Any smart card reader compliant with ISO 7816 and PC/SC standards supports usage of a secure channel.

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

A middleware or driver software is used for interacting with the TOE from application level. Aventra provides a minidriver for Microsoft Windows for interacting with the TOE. Authenticity of the minidriver can be verified by verifying its digital signature, which is attached into the executable. The minidriver is signed by a public certification authority which is normally trusted by the operating system. Alternatively, OpenSC open source smart card framework is used. In OpenSC, all changes are peer-reviewed before being accepted to the master branch of the repository. Anyone is free to review OpenSC's implementation. Secure processing of DTBS/R between the TOE and the application and integrity of DTBS/R can be ensured by using trusted middleware software.

Generation of DTBS/R from DTBS is done in application level. Applications must use a FIPS-140 or Common Criteria certified implementation of the hashing algorithm (for example, SHA-2) used to generate DTBS/R, or correct implementation of the algorithm must be verified by other means. Microsoft Windows and FIPS edition of BouncyCastle crypto library include FIPS-140 certified implementation of SHA-2 hashing algorithm and are safe choices, among other certified implementations.

A Security Specialist is required to consider compliance of the applications involved with this requirement.

5.2.6 OE.DTBS_Protect SCA protects the data intended to be signed

The TOE supports but does not require using a secure channel transferring DTBS/R from an application to the TOE. If a secure channel is not used, authenticity and trustworthiness of the application and middleware involved shall be considered by a Security Specialist.

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

Instructions or training must be provided for the Signatory to ensure awareness of importance of keeping their VAD confidential, and how to do so. Instructions shall be provided, on how to verify that the SCD is in non-operational state before verifying VAD.

5.2.8 OE.SCD/SVD_Auth_Gen Authorised SCD/SVD generation [PP3]

A Security Specialist is required to ensure that proper authentication and authorization is in place for invoking generation of the SCD and the SVD.

5.2.9 OE.SCD_Secrecy SCD Secrecy [PP3]

Generation of to-be-imported keys must be done in a secure environment. Guidance about key management is included in the Reference Manual in section 17.6. SCD to be imported can be generated either at the RA or at the CA. Archival of imported keys intended for the SSCD usage scenario is not allowed according to [PP3]. An imported SCD used for digital signature in the SSCD scenario must not be used outside the card for any signing or encryption purposes and must be deleted irreversibly after importing to the card.

A Security Specialist is required to review that this requirement is fulfilled in a particular usage scenario.

5.2.10 Uniqueness of the signature creation data [PP3]

Uniqueness of the signature creation data is ensured by using a certified implementation of the key generation algorithm. In practice, this can be accomplished by using for example Microsoft Windows' implementation of RSA or ECC key generation, which is FIPS 140-certified, FIPS certified edition of the Bouncy Castle crypto library or a CC or FIPS certified HSM device (where the key can be wrapped for transfer to the TOE), or other certified implementation.

5.2.11 OE.SCD_SVD_Corresp Correspondence between SVD and SCD [PP3]

Correspondance between SVD and SCD is ensured by using the Proof-of-possession scheme in certificate issuance: The certificate request is signed using the SCD, and the CA verifies the signature using the SVD which the certificate is requested for.

6 Configuration

This section contains descriptions how specific Security Functional Requirements (SFRs) are met in MyEID, and what must be considered to ensure each SFR is fulfilled, when configuring the card. Not all SFRs are listed, only those where additional explanation is considered necessary.

6.1 Cryptographic requirements

[SOGIS-ACM] defines that since December 31, 2025 the minimum acceptable key length for RSA is 3000 bits. This requirement shall be followed when using MyEID as CC EAL4+ compliant SSCD. As key length must be divisible by 64 with MyEID, the minimum allowed RSA key length is 3008 bits. This requirement is related to SFRs FCS_COP.1/RSA, FCS_CKM.1/RSA and FDP_ITC.1/SCD (key import).

6.2 SFRs

6.2.1 FDP_ACC.1/Signature_Creation Subset access control

To fulfil the requirements defined for Security attribute based access control defined as Signature Creation SFP in PP1, the following must be taken into account in personalisation:

- Subject S.User is the cardholder. The user is associated with the role R.Sigy, and technically this is ensured so that the user must authenticate a PIN code associated with the specific SCD (private key) to be used.

- SCD Operational: A private key has the attribute “SCD Operational”, when the MyEID card is in Operational State and the user has authenticated to the card with the associated PIN.

6.2.2 FDP_ACF.1/SCD/SVD_Generation_SFP Security attribute based access control

- When creating a Key EF, security attribute “Generate” can be set to an authentication object associated with user role R.Sigy or R.Admin. “Generate” security attribute corresponds to SCD/SVD Management, allowing the user generate a new key pair. Generate attribute can be given to R.Sigy or R.Admin, depending on usage scenario.

6.2.3 FMT_SMR.1 Security roles

- User roles are associated with authentication objects (PINs). R.Sigy is associated with PINs, which are associated with private keys. Typically, keys for different purposes are protected with separate PINs, so there may be several PINs for R.Sigy role. R.Admin is associated with SO-PIN, which is configurable and typically PIN #3 in MyEID applet. For EAL4+ certified usage, it is required to create separate PINs for R.Sigy and R.Admin roles.
- Use access condition of each Key EF must be set to the identifier of the correct authentication object.

6.2.4 FMT_SMF.1 Security management functions

- MyEID provides functions to initialise PIN codes for users and admin (PUT DATA: INITIALISE PIN)

6.2.5 FMT_MSA.1/Admin Management of security attributes

- Security attributes of a key cannot be changed after creation of a key file. Admin may have access to delete a key file.

6.2.6 FMT_MSA.1/Signatory Management of security attributes

- Only the user who possesses the PIN code associated with USE access condition of a specific private key has the ability to set the private key to operational state (SCD

operational). This can be done only by authenticating the associated PIN. To comply with this SFR, “Admin use key” flag shall not be set to the second status byte of the Proprietary Information field of a key EF.

6.2.7 FMT_MSA.2 Secure security attributes

- SCD/SVD Management can be assigned to both roles R.Admin and R.Sigy.
- The security attributes cannot be modified afterwards.
- MyEID supports generating keys in both preparative phase and operational phase.
- If keys are generated in preparative phase, the card is usually in Creation State. SCD/SVD Operational is set to “No” in Creation State. R.Sigy may or may not be given access to generate new keys later.
- Depending on security architecture of the operational environment, it can be considered safe to allow users generate new keys in Operational state. In this case, “Generate” attribute is set to an authentication object associated with R.Sigy.
- Customers should consider security requirements of their PKI, including security of the connection to a CA from workstations where key generation commands can be issued. Key generation can be restricted only to secure environments by not allowing users in role R.Sigy to create new Key EF’s, and by not associating “Generate” security attribute with R.Sigy.

6.2.8 FMT_MTD.1/Signatory

To comply with this SFR, **Allow admin changing and unblocking** and **Allow global unblocking** flags shall not be set for the PIN associated with the End user / R.Sigy role. This way, Administrator cannot change or unblock a user’s PIN.

6.2.9 FIA_AFL.1 Authentication failure handling

- MyEID internally counts failed authentication attempts and blocks PIN (RAD) after the counter exceed the configured maximum value.

6.2.10 FDP_UCT.1/SCD Basic data exchange confidentiality

- For using MyEID as an EAL4+ compliant SSCD, the user is required to use Secure Messaging when importing a private key using PUT DATA: LOAD KEY command.