Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1200-2026

for

Aventra MyEID PKI Smart Card, version 5.0.0

from

Aventra Oy

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1200-2026 (*)

Smartcards

Aventra MyEID PKI Smart Card, version 5.0.0

from	Aventra Oy
PP Conformance:	EN 419211-2:2013 - Protection profiles for secure signature creation device - Part 2: Device with key generation, BSI-CC-PP-0059-2009-MA-02, EN 419211-3:2013 - Protection profiles for secure signature creation device - Part 3: Device with key import, BSI-CC-PP-0075-2012-MA-01
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by AVA_VAN.5
valid until:	24 February 2031

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version CEM:2022 extended by Scheme Interpretations and by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version CC:2022. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL 2 and ALC_FLR
only

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 25 February 2026

For the Federal Office for Information Security

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

Fabian Hodouschek
Head of Certification

L.S.

Sandro Amendola
Director-General Directorate General S

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 87 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licensing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version CC:2022 [4] [1] also published as ISO/IEC 15408

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 2 December 2025, BGBI. 2025 , no. 301, p. 2

2 Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung – BSIZertV) of 02 December 2025, Bundesgesetzblatt 2025, no. 301

3 BMI Regulations on Ex-parte Costs – Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) – dated 2 September 2019, Bundesgesetzblatt I p. 1365

- Common Methodology for IT Security Evaluation (CEM), Version CC:2022 [2] also published as ISO/IEC 18045
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates – as far as such certificates are based on ITSEC or CC – under certain conditions was agreed.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2 and ALC_FLR components.

[4] Proclamation of the Federal Office for Information Security dated 14. April 2023 at https://www.bsi.bund.de.

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Aventra MyEID PKI Smart Card, version 5.0.0 has undergone the certification procedure at BSI.

The evaluation of the product Aventra MyEID PKI Smart Card, version 5.0.0 was conducted by SGS. The evaluation was completed on 25 February 2026. SGS is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Aventra Oy.

The product was developed by: Aventra Oy.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the evaluated guidance documentation, are observed,
- the product is operated in the environment as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis. Therefore the BSI reserves the right to revoke the certificate, especially if an exploitable vulnerability of the certified product gets to be known.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 25 February 2026 is valid until 24 February 2031. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

[5] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product Aventra MyEID PKI Smart Card, version 5.0.0, has been included in the BSI list of certified products, which is published regularly in the listing found at the BSI Website https://www.bsi.bund.de/dok/Zertifizierung-Gesamtlisten. Further information can be obtained from BSI-Infoline +49 (0)228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Aventra Oy
Lanttikatu 2
02770 Espoo
Finland

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of evaluation (TOE) is the product „Aventra MyEID PKI Smart Card, version 5.0.0“ by the vendor Aventra Oy. It is a composite product consisting of Aventra’s „MyEID“ Java Card applet version 5.0.0 running on top of the Common Criteria certified NXP JCOP4 Java Card operating system JCOP 4 P71 v4.7 R1.01.4 and JCOP 4 P71 v4.7 R1.02.4 (NSCIB-CC-2300127-02) [14] which itself comprises a Common Criteria certified NXP IC (BSI-DSZ-CC-1136-V5-2026) [17]. 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 Security Target [5] is the basis for this certification. It is based on the certified Protection Profiles EN 419211-2:2013 - Protection profiles for secure signature creation device - Part 2: Device with key generation, BSI-CC-PP-0059-2009-MA-02, EN 419211-3:2013 - Protection profiles for secure signature creation device - Part 3: Device with key import, BSI-CC-PP-0075-2012-MA-01 [7].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [5], chapter 6.1. They are all selected from Common Criteria Part 2. Thus the claimed set of SFRs in the ST is CC Part 2 conformant.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
SS.Signature Creation	The TOE provides a service to create signatures using RSA or ECC algorithms. For this it uses the cryptographic libraries provided by the platform.
SS.User Authentication	The TOE authenticates users using authentication objects, which can be either an alphanumeric PIN code or a challenge/response PIN.
SS.Data Decipherment	The TOE has capability to decipher data with a private key or with a symmetric secret key. The TOE uses platform’s functionality to perform data decipherment.
SS.Data Encipherment	The TOE has capability to encipher data with a private key or with a symmetric secret key. The TOE uses platform’s functionality to perform data encipherment.
SS.Key Generation	The TOE has capability to generate RSA and ECC keys pairs. The TOE uses platform’s functionality to perform key generation.
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.
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.
SS.Key Unwrapping	The TOE has capability to use its data decipherment feature to

TOE Security Functionality	Addressed issue
	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.
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.
SS.Key Agreement	The TOE has capability to generate a shared secret using ECDH algorithm. The TOE uses platform's functionality to perform the ECDH operation.
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.
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.
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.
SF.Applet Hardening	Applet hardening is implemented by applying nonbypassability and self-protection principles in the applet's code design, and by relying on the platform's features in domain separation, self-protection, emanation security and resistance to physical attacks using platform's services.
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.
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.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [5], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [5], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [5], chapter 3.4, 3.2 and 3.3.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 52, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification

Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

Aventra MyEID PKI Smart Card, version 5.0.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/SW	Aventra MyEID PKI Smart Card MyEID 5.0.0 running on JCOP 4 P71 v4.7 R1.01.4 and v4.7 R1.02.4	11/2024	Trackable shipment or collected from Aventra site.
2	DOC	Aventra Ltd. Aventra MyEID PKI Smart Card Reference Manual. Version 3.0.8. 02 2026	see left	Digitally signed electronic document (pdf) (https://aventra.fi)
3	DOC	Aventra Ltd. Aventra MyEID PKI Smart Card Reference Manual, Annex I - Common Criteria EAL4+ Compliance. Version 3.0.8. 01 2026	see left	Digitally signed electronic document (pdf) (https://aventra.fi)
4	DOC	Aventra Ltd. Getting Started with Aventra MyEID PKI Smart Card. Version 8.2. 08 2025	see left	Digitally signed electronic document (pdf) (https://aventra.fi)
5	Public Key	MyEID Factory Root Key	latest key on Aventra Oy website	x.509 certificate downloadable at Aventra web site (https://aventra.fi)
6	Public Key	MyEID Version Signing Key for MyEID 5.0.0, certified version	latest key on Aventra Oy website	x.509 certificate downloadable at Aventra web site (https://aventra.fi)

Table 2: Deliverables of the TOE

The delivery process is as follows:

• For the TOE itself (No. 1 in Table 2), the delivery will be shipped in an Aventra branded box. Integrity can be verified by checking the digital signature of the TOE as described in the user guidance [11].

• For documents and keys (No. 2 to 6 in Table 2), these can be downloaded on the developers website (https://aventra.fi). Verification has to be done by checking the digital signature of the PDFs. For keys, before downloading, care has to be taken to check the certificate of the Aventra website is valid and the TLS connection is secured. In case of doubt, Aventra shall be contacted for verification.

Identification of guidance documentation is clearly identified by version and released date, verified by the digitally signed PDFs.

The TOE itself consists of an applet pre-installed on a JCOP 4 P71 v4.7 R1.01.4 or R1.02.4 smart card. The TOE version is specified by the following configuration information:

MyEID PKI Smart Card	
Applet version:	MyEID 5.0.0 with "Security certification" bit set

Table 3: TOE reference

The information in Table 3 can be retrieved using APDU commands and has to be used by the user for identification. See [11] chapter 10 for guidance on TOE identification.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues: The TOE offers security services covering signature creation, user authentication, data decipherment, data encipherment key generation, key import, key wrapping, key unwrapping, secure key storage, key agreement, file management, authentication management and applet life cycle management, whereas the crypto functionality is provided by the certified platform. Additionally, the TOE offers security features covering applet hardening, platform security functionality and secure messaging.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

1. The CGA protects the authenticity of the signatory’s name or pseudonym and the SVD in the certificate by an advanced electronic signature of the CSP.

2. 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. The CSP uses only a trustworthy SCD/SVD generation device and ensures that this device can be used by authorised users 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.

Details can be found in the Security Target [5], chapter 4.3.

5. Architectural Information

The TOE consists of the MyEID applet version 5.0.0 on top of the certified platform JCOP 4 P71 v4.7 R1.01.4 and JCOP 4 P71 v4.7 R1.02.4 running on an underlying NXP IC.

The applet part of the TOE consists of one subsystem "MyEID applet", further split into several modules following the class structure of the applet. The SFR-enforcing modules are defined as follows:

- MyEID: Main processing logic, entry point for applet life cycle management and command processing.

- CryptoBuffer: Encapsulates binary data in a buffer, performs cryptographic operations on the encapsulated data.
- SecurityEnvironment: Maintains parameters of a Security Environment and contains implementations of commands related
- FileSystem: Contains an array of files, maintains the tree-like file structure and provides methods to access the files and enforce their access conditions.
- File: Contains properties and logic common to all files, include access condition list and file flags.
- BinaryFile: Represents a transparent file storing binary data.
- DirectoryFile: Represents a directory file that contains other files or directories.
- MasterDirectoryFile: Root directory, which is always present.
- KeyFile: Contains functionality and properties shared between all type of cryptographic key files.
- AsymmetricKeyFile: Contains functionality and properties specfic for any asymmetric cryptographic key file.
- GenericSecretFile, SecretKeyFile: Contains functionality and properties specfic for any symmetric cryptographic key file.
- RSAFile, EccFile, AesFile: Represents a RSA, ECC or AES key files stored on the certified platform.
- PinSlot: Representation and functionality for generic pin codes.
- ChallengeResponsePIN: Contains functionality and properties specfic for the challenge-response PIN used for authentication.
- AuthenticationSource: Represents a data source secured with a MAC, used for secure messaging.
- EncryptedSource: Represents an encrypted data source, used for secure messaging.
- PivCipherSuite: Implements the secure messaging for PIV, including key establishment and encryption and decryption of APDU commands with the help of the certified platform.
- PivEngine: Implements the mapping between the PIV data structures and the applets internal data structures.

Additional to the SFR-enforcing modules, the following SFR-supporting and SFR-non-interfering modules are defined: MyEIDProto, Message, BufferReader, SharedBuffer, EccDomain, Source, Sink, Composer, PivContainer, PivCcc, PivChuid, PivCertificate, Utilx.

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

7.1. ATE Testing

Developer Testing

The developer uses automated or code-driven testing approach. Two tools have been presented as part of the approach, Microsoft Minidriver Certification tool (CMCK) and, MyEID Tester, an in-house developed testing framework. This testing approach was applied to both hardware configurations as defined in the ST [5], MyEID 5.0.0 running on JCOP 4 P71 v4.7 R1.01.4 and JCOP 4 P71 v4.7 R1.02.4. Additionally, each of the configurations was tested with different settings, namely compatibility mode on and off for both, plain and secure messaging.

The tests are executed on a TOE in Creation State, after production and before delivery. Configuration steps are automated, providing a consistent testing state between the test runs. The developer tests focus on coverage of all TSFI as defined in the functional specification, consisting of both positive and negative testing. The sum of these tests cover both, intended functionality of the interfaces and the TOE itself, as well as TOE's ability to deal with unintended or incomplete input.

All actual results were reported as expected. The ITSEF deems the test concept presented by the developer to provide sufficient coverage and depth of the codebase.

Independent Testing

Overview:

The independent testing was partially performed using the developer's testing environment, partially using the test environment of the ITSEF.

All configurations of the TOE being intended to be covered by the current evaluation were tested.

The overall test result is that no deviations were found between the expected and the actual test results.

Independent testing approach:

Independent testing approach tests specific behaviours and characteristics of the TOE's interfaces found either explicitly mentioned in AGD_OPE documentation or as a result of ATE evaluation activities.

The testing approach exercises the interfaces of the TOE that trigger aforementioned behaviour of the TOE in order to verify the TOE's functionality is correct. This is achieved through exercising the APDU commands of relevant commands in order to trigger the behaviour to be tested.

TOE test configurations:

TOE running evaluated applet version, on two underlying platform revisions. Compatibility mode enabled, with testing of both plain and SM communication modes.

Independent test subset chosen:

The evaluator analysed the source code of the customer test tool to get an overview on coverage and depth of the already implemented test cases. Based on this analysis, they decided to implement 4 additional tests for independent testing that the evaluator deemed not sufficiently covered.

Developer’s test subset repeated:

The complete test suite of the developer of the MyEID Tester tool has been chosen for repeatability. Since the test suite of the developer is of an automated nature, effort on repeatability of these tests was minimal.

Verdict of the ITSEF:

The overall test result is that no deviations were found between the expected and the actual test results. Additionally, for the independent testing, all test results were as expected.

7.2. AVA Testing

Penetration testing was conducted on the two TOE configurations as defined in the ST[5], namely MyEID 5.0.0 running on JCOP 4 P71 v4.7 R1.01.4 and MyEID 5.0.0 running on JCOP 4 P71 v4.7 R1.02.4. The samples were identified, personalized and initialized as described in the user guidance ([9] and [12]).

During vulnerability analysis, the source code was analysed with focus on Man In The Middle attacks, replay attacks, denial of service attacks, authentication bypass attacks and SCA attacks. Additionally, the implementation of the APDU handling was checked in detail to verify that there are no issues in regards to undocumented or invalud APDU commands, invalid reads and invalid parameters.

As no applet specific vulnerabilities were discovered during the ITSEFs vulnerability analysis, the purpose of the tests was to assess the effectiveness of the countermeasures provided by the certified platform for perturbation attacks for protecting the TOE related assets, i.e. assessing that perturbation attacks are successfully identified and that an unauthorized updating of the content of a binary file is thereby prevented.

The ITSEF came to the verdict that penetration testing did not lead to any identifiable fault injection attack. It concluded the AVA_VAN work units with an overall “PASS”.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The two TOE configurations in scope of the evaluation are Aventra MyEID PKI Smart Card, version 5.0.0, based on platforms JCOP 4 P71 v4.7 R1.01.4 (contact-only) and v4.7 R1.02.4 (dual-channel)[14]. The difference in platform does not change the requirements, functionality or assumptions of the MyEID 5.0.0 applet.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [6] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL 5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4].

The following guidance specific for the technology was used:

(i) Attack Methods for Smartcards and Similar Devices,(see [4], AIS 26)

(ii) Application of Attack Potential to Smartcards,(see [4], AIS 26)

(iii) Minimum Requirements for Evaluating Side-Channel Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations (see [4], AIS 46)

(iv) Informationen zur Evaluierung von kryptographischen Algorithmen (see [4], AIS 46)

(v) Guidance for Smartcard Evaluation (see [4], AIS 37)

(vi) Composite product evaluation for Smart Cards and similar devices (see AIS 36). According to this concept the relevant guidance documents of the underlying platform and the documents ETR for Composition from the platform evaluations (i.e. on hardware [13, 14, 15, 16, 17, 18]) have been applied in the TOE evaluation.

(vii) Guidance for Tool-supported and automated software testing. Bundesamt für Sicherheit in der Informationstechnik. Version 1.0. Sept. 2021

(viii) 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. ENISA. Version 1. Feb. 2025

(ix) European Cybersecurity Certification Group Sub-group on Cryptography: Agreed Cryptographic Mechanisms. ECCG. Version 2.0. Apr. 2025

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: EN 419211-2:2013 - Protection profiles for secure signature creation device - Part 2: Device with key generation, BSI-CC-PP-0059-2009-MA-02,
  EN 419211-3:2013 - Protection profiles for secure signature creation device - Part 3: Device with key import, BSI-CC-PP-0075-2012-MA-01 [7]
- for the Functionality: PP conformant plus product specific extensions
  Common Criteria Part 2 conformant
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by AVA_VAN.5

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines the standard of application where its specific appropriateness is stated.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level	Comments
1	Key generation	Key generation: ECC	ISO 14888-3 [21, Section 6.6], ANSIX9-62 [22, Section 5.2], FIPS 186-5 [23, Section 6.2], SP800-186 [24, Section 3.2], RFC 5639 [25, Section 3]	256 to 521: P-256, P-384, P-521, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1 and brainpoolP512t1	≥ 120 bits [20, Section 4.3], [31, Section 2.3] Note: Brainpool curves having IDs ending with -t1 are isomorphic to the ones having IDs ending with -r1. The -t1 variants are not mentioned in [20] and [31], but these curves are implicitly included due to equivalency. See section 2.2 of [25].	FCS_CKM.1.1 / ECC
2	Authenticity, Integrity	Digital Signature Creation: ECDSA	ISO 14888-3 [21, Section 6.6], ANSIX9-62 [22, Section 5.3-5.4], FIPS 186-5 [23, Section 6.3-6.4], SP800-186 [24, Section 3.2], RFC 5639 [25, Section 3]	256 to 521: P-256, P-384, P-521, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1 and brainpoolP512t1	≥ 120 bits [20, Section 5.2], [31, Section 5.3.3, Section 2.3] Note: Brainpool curves having IDs ending with -t1 are isomorphic to the ones having IDs ending with -r1. The -t1 variants are not mentioned in [20] and [31], but these curves are implicitly included due to equivalency. See section 2.2 of [25].	FCS_COP.1 / ECC
3	Key	Key agreement:	SP800-56Ar3	256 to 521:	≥ 120 bits [20,	FCS_COP.1.1

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level	Comments
	agreement	ECDH	[26, Section 6], SP800-186 [24, Section 3.2], RFC 5639 [25, Section 3]	P-256, P-384, P-521, brainpoolP256r1, brainpoolP256t1, brainpoolP320r1, brainpoolP320t1, brainpoolP384r1, brainpoolP384t1, brainpoolP512r1 and brainpoolP512t1	Section 5.4], [31, Section 2.3.6, Section 2.3] Note: Brainpool curves having IDs ending with -t1 are isomorphic to the ones having IDs ending with -r1. The -t1 variants are not mentioned in [20] and [31], but these curves are implicitly included due to equivalency. See section 2.2 of [25].	/ ECDH
4	Key generation	Key generation: RSA	FIPS 186-5 [23, Section 5.1]	3008 to 4096 bit	≥ 120 bits [20, Section 7.3], [31, Section 5.3.1]	FCS_CKM.1 / RSA
5	Cryptographic primitive	RSA	PKCS#1 v2.2 (RFC8017) [27, Section 5]	3008 to 4096 bit	n/a	FCS_COP.1.1, FCS_COP.1.1 / Decipher
6	Authenticity, Integrity	Digital Signature Creation: RSA with PKCS#1 v1.5 padding	PKCS#1 v2.2 (RFC8017) [27, Section 8.2.1, Section 9.2]	3008 to 4096 bit	≥ 100 bits (Legacy) [20, Section 5.1], [31, Section 1.5]	FCS_COP.1.1
7	Authenticity, Integrity	Digital Signature Creation: RSA with PKCS#1 v2.2 PSS padding	PKCS#1 v2.2 (RFC8017) [27, Section 8.1.1, Section 9.1]	3008 to 4096 bit	≥ 120 bits [20, Section 5.2], [31, Section 5.3.1]	FCS_COP.1.1
8	Confidentiality	Decipher Operation: RSA with PKCS#1 v1.5 padding	PKCS#1 v2.2 (RFC8017) [27, Section 7.2.2]	3008 to 4096 bit	≥ 100 bits (Legacy) [20, Section 5.1], [31, Section 1.5, Section 2.3.2]	FCS_COP.1.1 / Decipher
9	Confidentiality	Operation: RSA with PKCS#1 v2.2 OAEP padding	PKCS#1 v2.2 (RFC8017) [27, Section 7.1.2]	3008 to 4096 bit	≥ 120 bits [20, Section 5.1], [31, Section 2.3.2]	FCS_COP.1.1 / Decipher

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level	Comments
10	Confidentiality	Encryption and Decryption: AES ECB, AES ECB (PKCS#7 padding)	FIPS 197 [28], SP800-38A [29, Section 6]	128, 192, and 256 bits	< 100 bits	FCS_COP.1 / AES ECB mode is not recommended; ECB is offered by the TOE, but there is a warning against using it in the user guidance [9, Section 17.4]
11	Confidentiality	Data Encryption and Decryption: AES CBC, AES CBC (PKCS#7 padding)	FIPS 197 [28], SP800-38A [29, Section 6]	128, 192, and 256 bits	≥ 120 bits [20, Section 2.1, Section 3.1], [31, Section 3.1]	FCS_COP.1 / AES, FDP_UCT.1 / SCD, FTP_ITC.1 / SCD
12	Authenticity, Integrity	Message authentication: AES-CMAC	FIPS 197 [28], SP800-38B [30, Section 6.2]	128, 192, and 256 bits	≥ 120 bits [20, Section 3.3], [31, Section 5.2]	FTP_ITC.1 / SCD

Table 4: TOE cryptographic functionality

Note: The TOE uses the RNG source of the certified platform (NSCIB-CC-2300172-02) [14].

The strength of the these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 52, Para. 4, Clause 2).

According to [20] and [31] the algorithms are suitable for the purposes as indicated in column “Purpose” of Table 4. An explicit validity period is not given.

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

11. Security Target

For the purpose of publishing, the Security Target [5] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

Conformity of the IT Product identified in this certificate with the Regulation (EU) No 910/2014 and Amendment Regulation (EU) 2024/1183 as well as the related scope and restrictions are stated in a separate document [14].

13. Definitions

13.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
APDU	Application Protocol Data Unit
DTBS/R	Data to be signed or its unique representation
CGA	Certification Generation Application
CSP	Certification Service Provider
SCA	Signature Creation Application
SCD	Signature Creation Data (refers to private or secret keys stored on the TOE for any cryptographic usage)
SVD	Signature Verification Data

13.2. Glossary

Augmentation – The addition of one or more requirement(s) to a package.

Collaborative Protection Profile – A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension – The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal – Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal – Expressed in natural language.

Object – A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package – named set of either security functional or security assurance requirements

Protection Profile – A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target – An implementation-dependent statement of security needs for a specific identified TOE.

Subject – An active entity in the TOE that performs operations on objects.

Target of Evaluation – An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality – Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation/CC
ISO-Version:
ISO 15408:2022, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities
- Part 5: Pre-defined packages of security requirements
https://www.iso.org/standard/72891.html
https://www.iso.org/standard/72892.html
https://www.iso.org/standard/72906.html
https://www.iso.org/standard/72913.html
https://www.iso.org/standard/72917.html
CCRA-Version:
CC:2022 R1, Common Criteria for Information Technology Security Evaluation
- Part 1: Introduction and general model
- Part 2: Security functional components
- Part 3: Security assurance components
- Part 4: Framework for the specification of evaluation methods and activities

- Part 5: Pre-defined packages of security requirement
https://www.commoncriteriaportal.org

[2] Gemeinsame Evaluationsmethodologie für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology
ISO-Version:
ISO 18045:2022: Information technology Security techniques Methodology for IT security evaluation
https://www.iso.org/standard/72889.html
CCRA-Version:
CEM:2022 R1, Common Methodology for Information Technology Security Evaluation
https://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licensing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7]
https://www.bsi.bund.de/AIS

[5] Security Target BSI-DSZ-CC-1200-2026, Version 1.17, 23.02.2026, Aventra MyEID PKI Smart Card Security Target, Aventra Oy.

[6] Evaluation Technical Report, Version 3.0, 23.02.2026, Evaluation Technical Report (ETR) – Summary, BSI-DSZ-CC-1200, Aventra MyEID PKI Smart Card, version 5.0.0, SGS Digital Trust Services GmbH, (confidential document).

[7] EN 419211-2:2013 - Protection profiles for secure signature creation device - Part 2: Device with key generation, BSI-CC-PP-0059-2009-MA-02

EN 419211-3:2013 - Protection profiles for secure signature creation device - Part 3: Device with key import, BSI-CC-PP-0075-2012-MA-01

[8] Configuration List, Version 1.0.10, 10.02.2026, MyEID CM scope (ALC_CMS) Configuration List, Hannu Honkanen (Aventra Oy).

[9] Aventra MyEID PKI Smart Card Reference Manual, Version 3.0.8, 02 2026, Aventra Ltd.

[7] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung
- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile für Evaluationen nach CC
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR für Evaluationen nach CC
- AIS 23, Version 4, Zusammentragen von Nachweisen der Entwickler
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[10] Aventra MyEID PKI Smart Card Reference Manual, Annex I - Common Criteria EAL4+ Compliance, Version 3.0.8, 01 2026, Aventra Ltd.

[11] Guidance_AGD Operational User Guide (AGD_OPE), Preparative procedures (AGD_PRE), Version 1.1.2, 02 2026, Aventra Ltd.

[12] Getting Started with Aventra MyEID PKI Smart Card, Version 8.2, 08 2025, Aventra Ltd.

[13] JCOP 4 P71 Security Target Lite for JCOP 4 P71, Version Rev. 4.17, 02 2026, NXP Semiconductors.

[14] JCOP 4 P71, versions JCOP 4 P71 v4.7 R1.00.4, JCOP 4 P71 v4.7 R1.01.4, JCOP 4 P71 v4.7 R1.02.4, JCOP 4 SE050 v4.7, R2.00.11, JCOP 4 SE050 v4.7 R2.03.11 Certification Report, NSCIB-CC-2300127-02, Version 1, 02 2026, TrustCB B.V.

[15] Evaluation Technical Report for Composition NXP “JCOP 4 P71” – EAL6+ (25-RPT-134), Version 3.0, 02 2026, SGS Brightsight.

[16] NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) Security Target Lite, BSI-DSZ-CC-1136-V5-2026, Rev. 3.4, 9 December 2025, NXP Semiconductors

[17] Certification Report BSI-DSZ-CC-1136-V5-2026 for NXP Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4), Version 1.0, 30.01.2026, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[18] Evaluation Technical Report for Composite Evaluation (ETR COMP) NXP Secure Smart Card Controller N7121 with IC Dedicated Software and Crypto Library (R1/R2/R3/R4) B1, BSI-DSZ-CC-1136-V5-2026, Version 4.0, 12 2025, TÜV Informationstechnik GmbH

[19] Certificate of Conformity pursuant to Article 29 (1), 39 (1) and Annex II of the Regulation (EU) No. 910/2014 for Aventra MyEID PKI Smart Card, version 5.0.0, Federal Office for Information Security (BSI), Version 1.0, 02 2026

[20] European Cybersecurity Certification Group - Sub-group on Cryptography - Agreed Cryptographic Mechanisms, ECCG, Version 2.0, April 2025

equals

SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms, Version 1.4 (non-published version)

https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en

[21] ISO/IEC 14888-3:2018, IT Security techniques — Digital signatures with appendix, Part 3: Discrete logarithm based mechanisms, Edition 4, 2018, ISO

[22] American National Standard X9.62, Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), November 2005, ANSI

[23] Federal Information Processing Standards Publication 186-5 (FIPS PUB 186-5), Digital Signature Standard (DSS), February 2023, U.S. Department of Commerce/National Institute of Standards and Technology (NIST)

[24] Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters, NIST Special Publication (SP) 800-186, February 2023, National Institute of Standards and Technology (NIST)

[25] M. Lochter, J. Merkle, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, RFC 5639, March 2010, IETF

[26] Recommendation for pair-wise key-establishment schemes using discrete logarithm cryptography, NIST Special Publication (SP) 800-56Ar3, April 2018, National Institute of Standards and Technology (NIST)

[27] Public-Key Cryptography Standards (PKCS) #1 / RFC 8017: RSA Cryptography Specifications, Version 2.2, November 2016, Kathleen Moriarty, Burt Kaliski, Jakob Jonsson and Andreas Rusch

[28] Advanced Encryption Standard (AES), Tech. rep. NIST FIPS 197, May 2003, National Institute for Standards and Technology (NIST)

[29] Recommendation for Block Cipher Modes of Operation: Methods and Techniques, NIST Special Publication (SP) 800-38A, October 2010, National Institute for Standards and Technology (NIST)

[30] Recommendation for Block Cipher Modes of Operation: the CMAC mode for Authentication, NIST Special Publication (SP) 800-38B, June 2016, National Institute for Standards and Technology (NIST)

[31] BSI TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellänge. Tech. rep. BSI TR-02102-1. Jan. 2026, Bundesamt für Sicherheit in der Informationstechnik

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria in its CCRA Documents can be followed:

- On conformance claim definitions and descriptions refer to CC:2022 part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC:2022 Part 3 chapter 6.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CCRA CC:2022 Part 5.
- On the assurance class ASE for Security Target evaluation refer to CC:2022 Part 3 chapter 9
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC:2022 Part 3 chapters 7 to 15
- The table 1 in CC:2022 part 5, Chapter 4.2 summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published as the CCRA Version at
https://www.commoncriteriaportal.org/cc/index.cfm

The CC are published as the ISO/IEC Version at
https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment

Annex B of Certification Report BSI-DSZ-CC-1200-2026

Evaluation results regarding development and production environment

The IT product Aventra MyEID PKI Smart Card, version 5.0.0 (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), CEM:2022 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version CC:2022.

As a result of the TOE certification, dated 25 February 2026, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1, ALC_COMP.1)

are fulfilled for the development and production sites of the TOE listed below:

a) Aventra Oy, Kutomotie 16, 4th floor, Helsinki Finland (Development and optional Personalisation)

b) For development and production sites regarding the underlying JCOP platform please refer to the Certification Report NSCIB-CC-2300127-02 ([14]).

c) For development and production sites regarding the underlying IC platform please refer to the Certification Report BSI-DSZ-CC-1136-V5-2026 ([17]).

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [5]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [5]) are fulfilled by the procedures of these sites.

Note: End of report