Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1216-2024

for

secunet eID PKI Suite Certified CA Kernel SC Version 3.0.0

from

secunet Security Networks AG

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-1216-2024 (*)

Certificate Issuing and Management Component

secunet eID PKI Suite Certified CA Kernel SC
Version 3.0.0

from	secunet Security Networks AG
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.2
valid until:	07 March 2029

SOGIS
Recognition Agreement

Common Criteria

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

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 3.1 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. 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.

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, 8 March 2024

For the Federal Office for Information Security

Sandro Amendola
Director-General

L.S.

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

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 und für Heimat (Federal Ministry of the Interior and Community)
- 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 licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408

1 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

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 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

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 3.1 [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 Bundesministerium des Innern und für Heimat of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

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 secunet eID PKI Suite Certified CA Kernel SC, Version 3.0.0 has undergone the certification procedure at BSI.

The evaluation of the product secunet eID PKI Suite Certified CA Kernel SC, Version 3.0.0 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 7 March 2024. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: secunet Security Networks AG.

The product was developed by: secunet Security Networks AG.

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 following report, are observed,
- the product is operated in the environment described, 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 at the date of certification. 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.

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 8 March 2024 is valid until 07 March 2029. 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 secunet eID PKI Suite Certified CA Kernel SC, Version 3.0.0 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 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] secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen
Deutschland

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 secunet eID PKI Suite Certified CA Kernel SC Version 3.0.0 provided by secunet Security Networks AG. The TOE is a CA (Certification Authority) Kernel that provides request, issuance, revocation, and overall management of certificates and certificate status information.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile[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 ALC_FLR.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 7. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
SF1.1 Audit message generation	The Audit (also called Audit system or Audit unit) logs the security-relevant events that were performed by the TOE. These events are either triggered internally or by external components/users via Java methods. That is the CA-Core logs amongst others every event and the appropriate event state, in the case that this event triggers a process of the CA-Core. The CA-Core generates audit messages for the following auditable events: ● Startup and shutdown of the audit functions and ● further security-relevant events These audit messages are sent to the Audit. If the audit trail is full the TOE shutdowns.
SF1.2 Audit trail protection	After audit message generation the Audit unit of the TOE generates uniquely identifiable audit messages, so called audit records. The Audit is able to associate each auditable event with the identity of the user that caused the event as the identity (UserIdentity) is contained in the audit record. The Audit is able to select the set of events to be audited from the set of all auditable events based on the following attributes contained in the audit record (see Section 12.2 of [6]: object identity (Module), user identity (UserIdentity) and event type (EventType). The TOE triggers that a set of these chronological ordered audit records (called audit trail) are periodically signed by means of a digital signature by the Hardware Security Module, resulting in a so called protected audit trail (see Sections 12.3 and 12.4 of [6]. This period is configurable. In order to protect audit messages against modification or deletion the Audit uses timestamps (OE.Time stamps) and sequence numbers.

[7]Even though it doesn’t claim conformance to it, this ST is heavily based on the PP “Certificate Issuing and Management Component” [8]

TOE Security Functionality	Addressed issue
	The Audit also triggers further cryptographic operations with HSM to protect the audit messages. The Audit needs three different cryptographic keys to protect the audit trails. It needs two asymmetric key pairs, one signature key pair (ASK) and one encryption key (AEK) and also one current symmetric trail record key (TRK). All these keys are generated within and stored on the HSM. The asymmetric keys are generated during the bootstrap process of the TOE (see Section 2.7 of [6]). Audit records and audit trails are stored via Java-API in the Adapter.
SF2 Management of the TSF	At the first startup the CA-Core has no configuration. Thus, the CA-Core must first be configured via the Java-API. The Administrator shall specify the acceptable set of certificate extensions. The CA-Core performs the same checks for Java configuration method as described in SF3.2. That is certificate validation, signature verification, challenge/identity check and role check. If all checks succeed, the Audit generates an audit log (see SF1.1) and the CA-Core triggers the generation of a new symmetric key within HSM (see SF6). Then the CA-Core triggers HMAC (RFC2104) protection (see SF6) of the configuration within HSM. Finally the CA-Core stores the HMAC protected configuration via Java-API to the Adapter. In order to prevent replay every change of a configuration requires that the CA-Core triggers the generation of a new symmetric key (see SF6) and the deletion of the formerly used symmetric key within HSM. If a configuration is needed during processing the CA-Core loads all information via Java-API from the Adapter. Then the CA-Core verifies the HMAC (see SF6). If HMAC verification fails the Audit generates an audit log record (see SF1.1) and the CA-Core does not further continue processing. If HMAC verification succeeds the CA-Core Job processing is continued.
SF3.1 Challenge Request and Response	In order to prevent replay the CA-Core triggers a challenge-response algorithm. In a first step the external component must request a challenge via Adapter from the CA-Core. The CA-Core then triggers generation of a challenge (10 Byte). The Environment's Deterministic Random Number Generator (DRNG) of the CA Card is used to generate the challenge. The CA-Core then stores the challenge with the user identification given in the request (it is possible to have more than one challenge per user at any given time) and sends the challenge back to the external component via Adapter. Now the external component may request Job processing via Adapter in a second step. A Job must contain amongst others the requested challenge and must be signed with the user's private key.
SF3.2 Remote Data entry Verification, Authorization and Challenge Verification	Before CA-Core starts a particular process it performs the following checks to ensure the integrity of the consigned Java method data: The CA-Core ● performs user certificate validation and the appropriate certificate chain validation, ● performs the signature verification with all consigned data, ● checks whether the given challenge and the signature identity matches a stored challenge/identity, and ● checks whether the role of the signature identity has the right to perform the requested process (for example creating a new certificate or a new certification revocation list). The security attribute role belongs to individual users. The allowed roles are: Administrator, Auditor and Officer. The right to modify configuration files and profiles and to modify the security attribute role is limited to Administrators.

TOE Security Functionality	Addressed issue
	If all checks succeed, the Audit generates an audit log record (see SF1.1) and starts request processing. If a check fails, the Audit generates an audit log record (see SF1.1) and the CA-Core does not start request processing.
SF4 Certificate and Certificate Status management	The TOE triggers generation of X.509 certificates and CRLs according to the standards X.509v3 and RFC 5280. In addition to this, the TOE also generates CVC for EAC e-Passport infrastructure according to the BSI TR-03110 standard. The TOE maintains via Adapter all issued certificates and their current state in a database, in order to serve status information. Status information of certificates is made available through CRLs and delta CRLs (RFC 5280).
SF4.1 Certificate Generation	In case of a certificate request the CA-Core ● validates the certificate request against the loaded CAProfile, ● triggers signature verification of the certificate request within HSM, ● transforms the CAProfile and merge it with the certificate request into a certification template, ● triggers signing of certificate template to generate a certificate within HSM (see SF6) and ● returns the new certificate via Java-API to the Adapter.
SF4.2 Certificate Revocation	In case of a certificate revocation list request the CA-Core ● merges the CRLProfile and the list of revoked certificates into the certificate revocation list template, ● triggers singing of the certificate revocation list template within the environment (CA Card) (see SF6) and ● returns the new certificate revocation list via Java-API to the Adapter.
SF4.3 Certificate Status Export	Issued CRLs are stored via Java-API in the Adapter.
SF5 Access Control	The TOE enforces the CIMC TOE Access Control Policy specified in Section 10.1 in [6]. The access to resources in the TOE is controlled using access control lists, based on: ● access rule – accept or decline access to a resource, ● resource – a resource to which access is controlled, ● user – an entity that have access rights to a resource, ● role – a role that a user is allowed to take on. Since access rules are defined on a role, so for a user to have access rights he must be assigned roles. When a controlled resource is accessed, the CA-Core verifies that the caller meets the appropriate access rules for the resource and, if not, denies access and generates an error. If there are no access rules associated to the resource, access is denied. The TOE access control system maps authentication information to a user entity. The entity is then associated to a role in order to acquire privileges.
SF6 Cryptographic Key Management	For cryptographic operations the TOE partly relies on its environment. An external key storage is used to generate key material, to store these keys and to execute cryptographic operations with them. In addition, the TOE implements some cryptographic primitives by itself. All in all, three entities are involved in the cryptographic implementation of the TOE: **The CA Card (environment)**

TOE Security Functionality	Addressed issue
	The CA Card generates, stores and allows the use of EC keys for a CA. The CA Card supports the algorithms as defined in Table 1 in [6]. The CA Card also holds an AES key that is used for encryption/decryption of audit trails, the data store in the environment and the encryption/decryption of the core configuration. Please note however that the CA Card is only used to generate these keys while the actual encryption and decryption is performed by the TOE. **The TOE** The TOE itself implements the cryptographic primitives as defined in Table 2 in [6] and securely deletes cryptographic keys if not longer used. The TOE also provides a hash base deterministic random number generator. It should be noted that [8] contains stipulations about the implementation of cryptographic primitives in the environment. These requirements are not met by the description in this Security Target. This is the main reason that this Security Target does not claim conformance to [8]. The integrity and authenticity of keys stored by the TOE in the environment is protected by the usage of a digital signature, namely of the digital certificate structure in which it has been included. Every time a public key (which is stored in form of a certificate) needs to be used to perform any cryptographic operation, its protective digital signature will be verified and, in case of failure, an audit log entry (see SF1.1) will be generated and the key will be marked as tampered with, becoming unusable for all types of operations. The TOE triggers or performs zeroizing private keys in the environment and within the TOE, if required. The TOE may trigger the cryptographic operations within its environment which includes amongst others all cryptographic operations required.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 11.1.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 4.1. 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 [6], chapter 4.3, 4.4 and 4.5.

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 9, 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:

secunet eID PKI Suite Certified CA Kernel SC, Version 3.0.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Certified CA Kernel SC (zip file) Secunet_eID_PKI_Suite_Certified-CAKernel-3_0_0.zip that contains the items from no. 2 – 9:	3.0.0	Delivered as download via secunet Download-Portal
2	SW	JAR archive with the Certified CA Kernel SC functionality, CertifiedCAKernel.jar SHA256 sum: 49be126b2c17bcba5cbae860f9a55bef5b52c429f30b723b2ed3575fd6a695a3	3.0.0	Contained within no. 1
3	SW	JAR archive with the SinacardHandler functionality, HSMHandlerSinacard.jar SHA256 sum: 4baf577b06be37889f72a66dba0f4207359fe2e69f6f1886b7c8b12f4ec0038f	3.0.0	Contained within no. 1
4	SW	Batch file with bootstrapping functionality for Windows, bootstrap.bat SHA256 sum: 5429697a7e211e9fc9ce54df0525813f360f18363c710a8b3172be72fe31b8d1	3.0.0	Contained within no. 1
5	SW	Shell file with bootstrapping functionality for Linux, bootstrap.sh SHA256 sum: 6cbb191551c066606e951c4e598d152e51e2079a0a85dd5bb4b37b303b0312d3	3.0.0	Contained within no. 1
6	SW	Public key for signature verification: Can be used for verification of the signature of the zip file (after verification of its fingerprint, see section 2.2), PublicSignatureKey.pem SHA256 sum: 4f3e5d2e1a733eb6ff12f8a0663e6e904b4c8e5cf8a7805eb773db7875643cbe	-	Contained within no. 1
7	DOC	Manual including API documentation Manual Certified CA Kernel.pdf [10], SHA256 sum: e3fcc7fac60ab1ba789a98e15588ea2197d00eb42094ed06c52f6d8a9da73e34 javadoc-cc.zip [11], SHA256 sum: 53f1ea14696ceb209dfb009a1e603b21cade7d72d3b4cde1c83ccb1e82d50cd2	3.6.6	Contained within no. 1

8	DOC	Release Notes [12] (information about TOE changes, Bugfixes etc.), ReleaseNotes.pdf SHA256 sum: 7ff5434cbf1d6eee2331e6c100a34fec13579e1752108e5b1f1be57cad8e2918	3.0.0	Contained within no. 1
9	DOC	Security Target [6] secunet eID PKI Suite Certified CA Kernel SC Security Target, Security Target Certified CA KernelSC.pdf SHA256 sum: fe25bba6300b16124c2bd89b77676cba331aeb90007a5249162c251f5fc85f2e	3.3.4	Contained within no. 1
10	DOC	Signature over ZIP file containing all previous items SHA256 sum: 7f851b4a1541a5b732e9b8e31939672870b06ffdde3f40b10f66ebfc694d71e0	-	The signature is not part of the zip file but delivered separately with the TOE download.

Table 2: Deliverables of the TOE

2.1. TOE Delivery

The eID PKI Certified CA Kernel SC is delivered in binary form as a signed zip file via download from the secunet download portal. The software used by the download portal is TS FileX version 1.2. The download portal enforces https with server authentication with a X.509 server certificate. The web server supports TLS 1.2.

The download file is uploaded onto the download server by the product manager, which is not possible without their authentication via their username and download server password. After successful upload the product manager gets an e-mail which contains the one-time customer password and the URL for the download portal which the customer uses to download the TOE. The ID for the download URL is automatically generated. One-time customer password, download URL and information about the TOE version are forwarded to the customer via e-mail. After the customer has downloaded the TOE, the download portal generates a notification e-mail and sends it to the product manager so they can retrace the download.

2.2. Identification of the TOE by the User

In section 11.3 of [10] it is explained in detail how to check the authenticity and integrity of the delivered items. For a first step, the signature of the zip-file must be checked. For this purpose, the user has to verify the signature with help of the delivered public key and the accompanying correct fingerprint.

The fingerprint of the key that can be used for verification of the integrity and authenticity of the delivered items is:

SHA-256: 5040af99068e11769776f4ed5b47394f6836b6f7796f34edd1668d55a206a4e5

The fingerprint can also be found in the Security Target [6]. If the fingerprint is not correct, the delivery procedure must be repeated in accordance with section 11.2 of [10]. In case the verification of the signature fails, the customer is not allowed to use the downloaded file and the delivery procedure must be repeated in accordance with 11.2 of [10].

The Version of the CertifiedCAKernelSC library can be obtained by opening the JAR-File with any archive tool. The version is printed in the file MANIFEST.MF (see [10], section 11.3).

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 implements logical security functionality in order to provide Registration Authority (RA) functionality to verify the information in the public key certificates and determine the certificate status and CA functionality to generate certificates and certificate status information as well as audit data generation according example CIMC-3 (single component) of CIMC PP [8][8]. Specific details concerning the above mentioned security functionalities can be found in sec. 7 of [6].

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:

- OE.Administrators, Officers and Auditors guidance documentation:
  Deter Administrator, Officer or Auditor errors by providing adequate documentation on securely configuring and operating the CIMC.
- OE.Auditors Review Audit Logs:
  Identify and monitor security-relevant events by requiring auditors to review audit logs on a frequency sufficient to address level of risk.
- OE.Authentication Data Management:
  Ensure that users change their authentication data at appropriate intervals and to appropriate values (e.g., proper lengths, histories, variations, etc.) through enforced authentication data management (Note: this objective is not applicable to biometric authentication data.)
- OE.Communications Protection:
  Protect the system against a physical attack on the communications capability by providing adequate physical security.
- OE.Competent Administrators, Officers and Auditors:
  Provide capable management of the TOE by assigning competent Administrators, Officers and Auditors to manage the TOE and the security of the information it contains. Only non-hostile people are entrusted with administrative tasks.
- OE.Cooperative Users:
  Ensure that users are cooperative so that they can accomplish some task or group of tasks that require a secure IT environment and information managed by the TOE.
- OE.CPS:
  All Administrators, Officers and Auditors shall be familiar with the certificate policy (CP) and the certification practices statement (CPS) under which the TOE is operated.

[8] Even though it does not claim conformance to it, this ST is heavily based on the PP “Certificate Issuing and Management Component” [8]

- OE.Detect modifications of firmware, software, and backup data:
  Provide integrity protection to detect modifications to firmware, software, and backup data.
- OE.Disposal of Authentication Data:
  Provide proper disposal of authentication data and associated privileges after access has been removed (e.g., Job termination, change in responsibility).
- OE.HSM[9]:
  The smart card in the environment (CA Card) that is used by the TOE shall only be used exclusively by the TOE. That is no other IT component is allowed to use the smart card.
- OE.Installation:
  Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security.
- OE.Lifecycle security:
  Provide tools and techniques used during the development phase to ensure security is designed into the CIMC. Detect and resolve flaws during the operational phase.
- OE.Malicious Code Not Signed:
  Protect the TOE from malicious code by ensuring all code is signed by a trusted entity prior to loading it into the system.
- OE.Notify Authorities of Security Issues:
  Notify proper authorities of any security issues that impact their systems to minimize the potential for the loss or compromise of data.
- OE.Object and data recovery free from malicious code:
  Recover to a viable state after malicious code is introduced and damage occurs. That state must be free from the original malicious code.
- OE.Operating System:
  The operating system used is validated to provide adequate security, including domain separation and non-bypassability, in accordance with security requirements recommended by the National Institute of Standards and Technology.
- OE.Periodically check integrity:
  Provide periodic integrity checks on both system and software.
- OE.Physical Protection:
  Those responsible for the TOE must ensure that the security-relevant components of the TOE and non-TOE are protected from physical attack that might compromise IT security.
- OE.Preservation/trusted recovery of secure state:
  Preserve the secure state of the system in the event of a secure component failure and/or recover to a secure state.
- OE.Procedures for preventing malicious code:
  Incorporate malicious code prevention procedures and mechanisms.
- OE.Repair identified security flaws:
  The vendor repairs security flaws that have been identified by a user.
- OE.Require inspection for downloads:
  Require inspection of downloads/transfers.

[9] Even though the CA Kernel SC does not use a HSM, the name of the OE was kept out of convenience.

- OE.Security-relevant configuration management:
  Manage and update system security policy data and enforcement functions, and other security-relevant configuration data, to ensure they are consistent with organizational security policies.
- OE.Social Engineering Training:
  Provide training for general users, Administrators, Officers and Auditors in techniques to thwart social engineering attacks.
- OE.Sufficient backup storage and effective restoration:
  Provide sufficient backup storage and effective restoration to ensure that the system can be recreated.
- OE.Time stamps:
  Provide time stamps to ensure that the sequencing of events can be verified.
- OE.Trusted Path:
  Provide a trusted path between the user and the system. Provide a trusted path to security-relevant (TSF) data in which both end points have assured identities.
- OE.Validation of security function:
  Ensure that security-relevant software, hardware, and firmware are correctly functioning through features and procedures.
- OE.Cryptographic functions:
  Provide algorithms for authentication and signature generation/verification; key generation techniques. Please refer to chapter 1.2.1.1 of [6] for more details on the required algorithms.

Details can be found in the Security Target [6], chapter 5.2.

5. Architectural Information

The TOE is a CA (Certification Authority) Kernel that provides request, issuance, revocation, and overall management of certificates and certificate status information. The secunet eID PKI Suite Certified CA Kernel SC supports Extended Access Control Certification Authorities (EAC CAs,) according Technical Guideline BSI TR-03110 and International Civil Aviation Organization CAs (ICAO CAs), which are X.509 CAs according ITU-T X.509. For cryptographic operations the secunet CA Kernel SC relies on a smartcard in the environment as well as cryptographic functionality implemented by the TOE itself.

The Certified CA Kernel SC provides Registration Authority (RA) functionality as well as CA functionality according the CIMC PP [8].

The security functions of the TOE are:

- SF1 Security Audit
  - SF1.1 Audit message generation
  - SF1.2 Audit trail protection
- SF2 Management of the TSF
- SF3 Data Authenticity and Authorization
  - SF3.1 Challenge Request and Response

  - SF3.2 Remote Data entry Verification, Authorization and Challenge Verification
- SF4 Certificate and Certificate Status management
  - SF4.1 Certificate Generation
  - SF4.2 Certificate Revocation
  - SF4.3 Certificate Status Export
- SF5 Access Control
- SF6 Cryptographic Key Management

According to the TOE design specification these security functions are enforced by the following subsystems:

- System (supports the TSF SF1, SF2, SF3, SF4, SF5, SF6)
  - The subsystem System provides methods for the subsystems Audit, CACore and supports Bootstrap for the secure initialization.
- Audit (supports the TSF SF1)
  - Audit interacts with the subsystem system and provides message generation and protect Audit trails
- CA-Core (supports the TSFs SF2 and SF4)
  - The subsystem CA-Core interacts with the subsystem System and provides the main functionalities of the TOE
- Bootstrapping
  - The subsystem bootstrapping interacts with subsystem System and CA-Core, to ensure a secure initialization and boot process on the first initialization of the TOE.

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. Test Summary

The developer tested all TOE security functions. For all commands and functionality tests, test cases were specified in order to demonstrate its expected behaviour including error cases. Hereby a representative sample including all boundary values of the parameter set were tested and all functions were tested with valid and invalid inputs. Repetition of developer tests were performed during the independent evaluator tests.

During their testing, the evaluators covered

- Testing of all developer tests and
- additional evaluator tests

- Vulnerability analysis

The evaluators have tested the TOE systematically against enhanced basic attack potential during their testing.

The achieved test results correspond to the expected test results.

7.2. Developer Testing

TOE test configuration

The TOE was tested in the secunet testing environment in two ways: In the lab environment the TOE was installed on a standard PC fulfilling the requirements from chapter 1.2.3 of [6]. It was connected to multiple card readers which contained the CA Cards. The CA Cards used for developer testing were the Javacard and the STARCOS 3.5 card in the testing scenario with real cards and the STARCOS 3.5 card in the testing scenario with virtual cards. This environment was tested using the operating system RedHat Enterprise 7. In the virtual environment the TOE was run on a virtual machine (VirtualBox) with virtual smartcards and a key file as a PIN pad substitute. These tests were conducted using all four operating systems (RedHat 7, RedHat 8, Windows Server 2016, Windows Server 2019). Besides the requirements described in chapter 1.2.3 of [6] the test environment also needed to fulfil the security objectives for the environment. The TOE environment and the related test equipment for the tests were consistent with the described ones in [6] and [10].

The developer test configuration for the virtual environment and the test protocols were provided to the evaluator.

Testing approach

The developer specified and implemented test cases for each defined subsystem. The test cases are divided into tests of the CA-Core, Audit, System, Bootstrapping and Miscellaneous. Thus all subsystems are covered by several test cases.

For the tests of the TOE the developer used the JUnit testing framework. In this framework test cases are implemented in Java. Each test is implemented as a Java method. The tests can be run and the frameworks shows whether the test was successful. To create extensive log files as required for the evaluation the developer changed the default behaviour of the testing framework, so additional information about the testing is logged.

Testing Results

The results of the TOE tests suggest a correct implementation. All test cases were executed successfully and ended up with the expected result.

7.3. Independent Evaluator Tests

Overview

The independent testing was performed using the developer’s test software environment.

The configuration of the TOE being intended to be covered by the current evaluation was tested.

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

Since the evaluator used the test environment of the developer, there was no deviation between the developer test configuration and the evaluator test configuration.

The description of the required non-TOE hardware, software and firmware is described in section 1.2.3 of [6]. Note that the developer conducted testing on all four supported operating systems (RedHat 7, RedHat 8, Windows Server 2016, Windows Server 2019). The evaluators repeated as a test sample all developer tests in the virtual test environment with the simulated STARCOS 3.5 CA card on the operating system RedHat 8.

The entire developer test configuration and the test protocols were provided to the evaluator.

Test Configuration

The evaluator used the same TOE test configuration as the developer, so the statement from “TOE test configuration” above applies.

The description of the required non-TOE hardware, software and firmware is described in chapter 1.2.3 of [6]. The following configuration was the configuration of the virtual machine test setup:

- Smartcard Emulator: STARCOS 3.5
- RedHat 8 Operating System

For the tests of the TOE which were carried out at the evaluator’s site this configuration was used.

The virtual test network used by the evaluators was only implemented with the VirtualBox with RedHat Enterprise Version 8. One of the key features of Java is the abstraction of the execution of the TOE from the operating system platform via the Java Virtual Machine, so the direct execution environment is the JVM with its interface to the operating system. Therefore the Java application behaves exactly the same, if no operating system specific parameters libraries or frameworks are used, which is not the case for the TOE. Another way to force a different behaviour on different operating system is by using the functions provided by the System java class. To query the OS on which the JVM runs, the query System.getProperty("os.name") can be added to the source code of a product that is not tailored to a specific operating system platform. The query System.getProperty("*") is used only twice in the delivered source code:

- In the Test Suite (AbstractHSMSettings and TestUser), but the Test Suite is not part of the TOE.
- In file BootstrapHandler: During bootstrapping, the user directory of the current user is determined via the query System.getProperty("user.dir"). Access to the user directory is executed via the JVM and therefore platform-independent.

The evaluators checked the source code for these queries and found only the two instances mentioned above. Therefore they came to the conclusion that the TOE is platform-independent and therefore virtual testing of the TOE on only one platform is sufficient.

The TOE was tested by the evaluators using the virtual secunet testing environment with the specifications mentioned above, on a virtual machine image with RedHat Enterprise Linux 8 and a STARCOS 3.5 Smartcard Simulator.

The developer provided the log files of his testing with the real smartcards, therefore the evaluators could verify that their test environment acts as the TOE environment.

Subset size chosen

As a chosen test subset the evaluators repeated all developer tests in the virtual test environment with the simulated STARCOS 3.5 CA Card on the operating system RedHat 8.

Independent test subset chosen incl. a short justification:

The independent test subset consisted of seven individual tests. Each SFR-enforcing TSFI was tested at least once. The following tests were conducted:

- The method changeCertificateStateAndDelete() is called on a Certificate with a signature signed for another Certificate.
- The TOE must not allow commands other than getState in its secure state AuditError.
- The TOE does not create a new CA.
- After a manipulation of a trail the TOE goes into AuditError state. The audit logs can only restored by an administrator, not by the role officer.
- The TOE must not start with an incorrect system configuration.
- Two consecutive trails are being corrupted (which is not possible under normal operation). The method fixTrailStorage() is called first without the flag “forceInitialisation” and then with the flag.
- The TOE creates two certificates and performs various changes on the states of the two certificates.

For all evaluator tests the actual result matched the expected result and thus the tests were executed successfully.

Developer’s test subset repeated incl. a short justification:

All developer tests were repeated by the evaluators. In all test cases the expected result was met.

Verdict for the sub-activity:

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

Vulnerability analysis

The evaluator applied a methodical analysis to create a list of potential vulnerabilities. The evaluators have conducted their search and have taken the following information into account: All evaluation deliverables, in particular the ST and the deliverables for classes ADV, AGD, ALC and ATE.

First, the evaluator created a list of potential vulnerabilities based on the results gained while performing the vulnerability analysis. This list merely considered the current TOE type / TOE specific technology / TOE specific implementation, but not its intended operational environment. No further vulnerabilities were identified.

Secondly, the evaluator reconstructed the formal assumptions about the TOE operational environment. In order to do this he referred to [6], section 5.1 and 5.2. The operational environment does neither restrict nor extend vulnerabilities.

Having performed the analysis above, the evaluator found no remaining potential vulnerabilities that may be exploitable in the intended TOE environment with the attack potential enhanced basic.

During the vulnerability analysis of the evaluator all potential attack methods and vulnerabilities were discussed in a systematic way in accordance to the attack potential enhanced basic.

According to the CEM [2] there must be a penetration test analysis for identified potential vulnerabilities. Due to the fact that there are no potential vulnerabilities identified that are not analysed in AVA there was no further penetration testing done by the evaluator.

The evaluators took the following approach to perform the vulnerability assessment of the TOE. First the evaluators verified that the TOE configuration matches the one described in the ST [6]. After that, the evaluators verified that the TOE is in a known state.

The evaluators examined publicly available information to find hints for potential vulnerabilities in the TOE. This included gathering information about the TOE type and common attacks against it as well as collect CVEs of the libraries used in the TOE and the environment. Then the evaluators conducted a focused search of ST, guidance and all other developer deliverables for the various evaluation aspects, to find potential vulnerabilities. The evaluators searched for common implementation flaws for Java-based applications. The advices in the OWASP TOP 10 for Java EE Guide and the CWE Weaknesses Guide have been considered when reviewing the source code of the TOE. Additionally the source code was verified using a static code analysis tool to detect common errors.

None of these activities led to the need of additional penetration tests. Therefore, the evaluators have performed no penetration tests.

The test results fulfil the requirements of AVA_VAN.3.

8. Evaluated Configuration

This certification covers the following evaluated configuration, defined by the notation:

- secunet eID PKI Suite Certified CA Kernel SC
- The documents:
  - Handbuch [10]
  - Release Notes [12]
  - Security Target [6]

To identify the TOE as outlined in chapter 2.1 of the ST [6], the Guidance [10] is providing sufficient information in chapter 12.

The description of the required non-TOE hardware, software and firmware is described in chapter 1.2.3 of [6]. The requirements for the non-TOE hardware, software and firmware are the following:

CA-Server

- 4096 MB RAM
- 2.4 GHz CPU (64 bit)
- 64 GB storage

The hardware must be compatible with the JVM (see [6], section 1.2.3.2). The physical connections are:

- Network Card

- Power Supply
- PS/2- or USB-attached keyboard
- VGA graphics adapter
- Card reader

JVM

The Certified CA Kernel SC is implemented in Java. Thus, it interacts with the interfaces of the Java Virtual Machine instead of directly interacting with the underlying operating system. The Certified CA Kernel SC requires the following JVM being present in its environment:

- Oracle JVM 17

Operating System

While the use of the JVM as a universal interface allows the Certified CA Kernel SC to operate under all operating systems that allow the operation of the aforementioned JVMs, it is recommended to utilize an operating system that provides adequate security measures and is actively maintained. Specifically, the Certified CA Kernel SC is tested for operation under the following OS:

- Windows Server 2016 and 2019,
- Red Hat Enterprise Linux 7 and 8 or Rocky Linux 8 (which is equivalent to RHEL 8)

The CA Card used as part of the crypto module shall fulfil the following requirements:

1) Provide the required functionality as needed for the use case and as identified in table 1 of the ST [6]

2) Provide sufficient trust into the implementation. This can e.g. be shown by using a certified card (on at least the assurance level from this certification).

As an example, the Giesecke und Devrient STARCOS 3.5 on Infineon SLE78CLX1280P (M7820A11) could be used.

The systems used by the evaluators during the testing fulfils these requirements.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] 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.

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 ALC_FLR.2 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: None.
- for the Functionality: Product specific Security Target
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_FLR.2

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 strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context) only.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Audit Trail security	RSA key generation	PKCS#1/ FIPS 186-5 [13]	2048, 3072	yes	
2	Audit Trail security	RSA encryption/decryption RSAES-OAEP	PKCS#1/ FIPS 186-5 [13]	2048, 3072	yes	
3	Audit Trail security Certificates	RSA signature creation ● RSA_SHA256_PKCS1 ● RSA_SHA384_PKCS1 ● RSA_SHA512_PKCS1 ● RSA_SHA256_PSS ● RSA_SHA384_PSS ● RSA_SHA512_PSS	PKCS#1/ FIPS 186-5 [13]	2048, 3072	yes	
4	Audit Trail security Certificates	RSA signature verification ● RSA_SHA256_PKCS1 ● RSA_SHA384_PKCS1 ● RSA_SHA512_PKCS1 ● RSA_SHA256_PSS	PKCS#1/ FIPS 186-5 [13]	2048, 3072	yes	

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
		● RSA_SHA384_PSS ● RSA_SHA512_PSS				
5	Verification of signatures	ECDSA signature verification	BSI TR-03111 [14]	supported elliptic curves: ● NIST-P224/ secp224r1 ● NIST-P384/ secp384r1 ● NIST-P512/ secp512r1 ● NIST-P256/ secp256r1 ● NIST-K233/ sect233k1 ● NIST-B233/ sect233k1 ● NIST-K283/ sect283k1 ● NIST-B283/ sect283r1 ● NIST-K409/ sect409k1 ● NIST-B409/ sect409r1 ● NIST-K571/ sect571k1 ● NIST-B571/ sect571r1 ● brainpoolP256r1 ● brainpoolP256t1 ● brainpoolP320r1 ● brainpoolP320t1 ● brainpoolP384r1 ● brainpoolP384t1 ● brainpoolP512r1 ● brainpoolP512t1	yes	
6	Verification of signatures	ECGDSA signature verification	BSI TR-03111 [14]	supported elliptic curves: ● NIST-P224/ secp224r1 ● NIST-P384/	yes	

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
				secp384r1 ● NIST-P512/ secp512r1 ● NIST-P256/ secp256r1 ● NIST-K233/ sect233k1 ● NIST-B233/ sect233k1 ● NIST-K283/ sect283k1 ● NIST-B283/ sect283r1 ● NIST-K409/ sect409k1 ● NIST-B409/ sect409r1 ● NIST-K571/ sect571k1 ● NIST-B571/ sect571r1 ● brainpoolP256r1 ● brainpoolP256t1 ● brainpoolP320r1 ● brainpoolP320t1 ● brainpoolP384r1 ● brainpoolP384t1 ● brainpoolP512r1 ● brainpoolP512t1		
7	Encryption and decryption of secrets	AES key generation	FIPS197 [15]	128, 256	yes	
8	Audit Trail Security	AES HMAC_SHA256 RFC2104	SP 800-38B [17]	128, 256	yes	
9	Encryption and decryption of secrets	AES encryption/decryption with CBC and PKCS5 Padding	SP 800-38A [17]	128, 256	yes	

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
10	Hashing for various functions	SHA-256 SHA-1[10]	FIPS180-2 [16]	256, 384, 512	SHA-1: no, SHA-256: yes	

Table 3: TOE cryptographic functionality

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.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AEK Asymmetric Encryption Key

ASK Asymmetric Signature Key Pair

AIS Application Notes and Interpretations of the Scheme

[10] It is important to mention that the SHA-1 is only used to derive a fingerprint and to support legacy PKI systems that have been set up using SHA-1.

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
CA	Certification Authority
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CIMC	Certificate Issuing and Management Component
CP	Certificate Policy
CPS	Certification Practices Statement
cPP	Collaborative Protection Profile
CRL	Certificate Revocation List
CVC	Card Validation Code
CVE	Common Vulnerabilities and Exposures
EC	Elliptic Curve
EAC	Extended Access Control
DRNG	Deterministic Random Number Generator
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HMAC	Hashing for Message Authentication
HSM	Hardware Secure Module
ICAO CA	International Civil Aviation Organization Certification Authority
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
ITU-T	ITU Telecommunication Standardization Sector
JAR	Java Archive
PKI	Public Key Infrastructure
PP	Protection Profile
RA	Registration Authority
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TRK	Symmetric Trail Record Key
TSF	TOE Security Functionality

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.

Semiformal - Expressed in a restricted syntax language with defined semantics.

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, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017,
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 licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[11]
https://www.bsi.bund.de/AIS

[11] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-1216-2024, Version 3.3.4, 20.02.2024, secunet eID PKI Suite Certified CA Kernel SC Security Target, secunet Security Networks AG

[7] Evaluation Technical Report, Version 1.3, 07.03.2024, Evaluation Technical Report (ETR) – Summary, SRC Security Research & Consulting GmbH, (confidential document)

[8] Certificate Issuing and Management Components Protection Profile Version 1.5, 11 August, 2011, Communications Security Establishment Canada, Document number: 383-6-3-CR

[9] Configuration list for the TOE, Version 1.3.9, 07.03.2024, Konfigurationsliste ALC_CMS.4, cms_secunet+eID+PKI+Suite_V.1.3.9.pdf, secunet Security Networks AG (confidential document)

[10] Guidance documentation for the TOE, Version 3.6.6, 20.02.2024, Handbuch (AGD_PRE.1 und AGD_OPE.1), agd_secunet+eID+PKI+Suite_v3.6.6.pdf, secunet Security Networks AG

[11] API Documentation (JavaDoc), Version 3.6.6, 20.02.2024, javadoc-cc.zip, secunet Security Networks AG

[12] Release Notes, Version 3.0, 15.01.2024, ReleaseNotes.pdf, secunet Security Networks AG

[13] FIPS PUB 186-5: Digital Signature Standard (DSS) / National Institute of Standards and Technology (NIST), February 2023

[14] TR-03111 Technical Guideline TR-03111 – Elliptic Curve Cryptography,; Version 1.11, April 2009 / Bundesamt für Sicherheit in der Informationstechnik (BSI)

[15] Advanced Encryption Standard (AES), FIPS 197, November 26, 2001

[16] Secure Hash Standard (SHS), 8/04/2015

[17] NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques; and NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication

C. Excerpts from the Criteria

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

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report