Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1144-2021

for

secunet eID PKI Suite Certified CA Kernel, Version 2.0.3

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-1144-2021 (*)

Certificate Issuing and Management Component

secunet eID PKI Suite Certified CA Kernel
Version 2.0.3

from	secunet Security Networks AG
PP Conformance:	Certificate Issuing and Management Components Protection Profile Version 1.5, 11 August, 2011, Communications Security Establishment Canada, Document number: 383-6-3-CR
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.2

SOGIS
Recognition Agreement

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.

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

Bonn, 15 January 2021

For the Federal Office for Information Security

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

Sandro Amendola L.S.
Head of Division

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 licencing process (CC-Stellen) [3]

[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 Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.
- 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.

[4] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

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

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, Version 2.0.3 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0960-2015. Specific results from the evaluation process BSI-DSZ-CC-0960-2015 were re-used.

The evaluation of the product secunet eID PKI Suite Certified CA Kernel, Version 2.0.3 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 11 January 2021. 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 15 January 2021 is valid until 14. January 2026. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

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,
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, Version 2.0.3 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
Weidenauer Straße 223-225
57076 Siegen

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 Version 2.0.3 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 based on the certified Protection Profile Certificate Issuing and Management Components Protection Profile Version 1.5, 11 August, 2011, Communications Security Establishment Canada, Document number: 383-6-3-CR [8].

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 6. 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.
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. 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. This period is configurable. In order to protect audit messages against modification or deletion the Audit uses timestamps and sequence numbers. The Audit also triggers further cryptographic operations with HSM to protect the audit messages.
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 following checks for Java

TOE Security Functionality	Addressed issue
	configuration method: certificate validation, signature verification, challenge/identity check and role check. In order to prevent replay, every change of a configuration requires that the CA-Core triggers the generation of a new symmetric key and the deletion of the formerly used symmetric key within the HSM. Then the CA-Core triggers HMAC verification within the HSM. If HMAC verification fails the Audit generates an audit log record 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) within HSM. The HSMs Deterministic Random Number Generator (DRNG) 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. If all checks succeed, the Audit generates an audit log record and starts request processing. If a check fails, the Audit generates an audit log record 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.
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,

TOE Security Functionality	Addressed issue
	● 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 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 HSM 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. 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 relies on a FIPS 140-2 Level 3 certified or a CC certified cryptographic module – a Hardware Security Module (HSM) – according to the Certificate Issuing and Management Components (CIMC) Protection Profile [8]. All cryptographic operations (key generation, hashing, signing, verifying and key zeroizing) are performed within this validated cryptographic module. Of course, the TOE triggers all cryptographic operations of the HSM. The TOE only manages Component keys. Component keys are used to sign certificates and certificate status information. Component keys are also used to sign audit logs and to ensure the integrity of changed Jobs by CA-Core. Component private keys are only stored on the HSM. The integrity and authenticity of public keys stored by the TOE on the database – outside the HSM – 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 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 will be generated and the key will be marked as

TOE Security Functionality	Addressed issue
	tampered with, becoming unusable for all types of operations. The TOE triggers zeroizing plaintext Component private keys within the HSM, if required. The TOE may trigger the following cryptographic operations within the HSM: ● Generate Key ● Crypt Data ● Sign Data ● Verify Signature ● Compute Hash ● Agree Secret ● Generate Random Number

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 10.1.

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 to 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, Version 2.0.3

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Certified CA Kernel (zip file) that contains the items from no. 2 – 9, secunet_eID_PKI_Suite_CertifiedCAKernel-2_0_3.zip	2.0.3	Delivered as download via secunet Download-Portal.
2	SW	JAR archive with the Certified CA Kernel functionality, CertifiedCAKernel.jar SHA256 sum: f85a4c4aed36bb044b8e3460ab9048616338e6749295166d33f54947b570c5a6	2.0.3	Contained within no. 1.
3	SW	Batch file with bootstrapping functionality for Windows, bootstrap.bat SHA256 sum: 5429697a7e211e9fc9ce54df0525813f360f18363c710a8b3172be72fe31b8d1	2.0.3	Contained within no. 1.
4	SW	Shell file with bootstrapping functionality for Linux, bootstrap.sh SHA256 sum: 6cbb191551c066606e951c4e598d152e51e2079a0a85dd5bb4b37b303b0312d3	2.0.3	Contained within no. 1.
5	SW	Public key for signature verification[7], PublicSignatureKey.pem SHA256 sum: 5040af99068e11769776f4ed5b47394f6836b6f7796f34edd1668d55a206a4e5	-	Contained within no. 1.
6	DOC	Manual [10], Certified CA Kernel Manual.pdf SHA256 sum: a20597aac0baa3c1c6e4b958f382ecd71c9ccc68282c265611798c3c354a1806	3.4.6	Contained within no. 1.
7	DOC	API documentation [11], javadoc.cc.zip SHA256 sum: 241234358226a06e0baccb0ceba7c241df8562d7136cc1c6e76fc055718bdbd5	3.4.6	Contained within no. 1.
8	DOC	Release Notes [12], ReleaseNotes.pdf SHA256 sum: 7d358f42a858505043ffc422fb8bff8bab8cd7ee127af283565ef27d26c51860	2.0.3	Contained within no. 1.

[7] To be used for verification of the signature of the ZIP file (after verification of its fingerprint, see #10).

No	Type	Identifier	Release	Form of Delivery
9	DOC	Security Target [6], st_secunet eID PKI Suite Certified CA Kernel_v3.1.6.pdf SHA256 sum: e707b6a7836c265fbde654f42f61325ce221dacc ee2393d602e6e138a73490b4	3.1.6	Contained within no. 1.
10	SIG	Signature over ZIP file containing all previous items, secunet_eID_PKI_Suite_CertifiedCAKernel-2_0_3.zip.sha256	-	The signature is not part of the ZIP file but delivered separately.

Table 2: Deliverables of the TOE

2.1. TOE Delivery

The eID PKI Certified CA Kernel is delivered in binary form as a signed .zip file via download from the secunet download portal. 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. 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. 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 authenticity and integrity of 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 integrity and authenticity of the delivered items is:
5040af99068e11769776f4ed5b47394f6836b6f7796f34edd1668d55a206a4e5 (SHA-256)

The fingerprint can also be found in the Security Target. If the fingerprint does not match, the delivery procedure must be repeated in accordance with section 11.3 of [10]. In case the verification of 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 TOE can be obtained by opening the file CertifiedCAKernel.jar (item 2 of the table above) with any archive management tool. The JAR-file contains the file MANIFEST.MF in the subfolder “META-INF/” of the archive. This file contains several properties of the JAR-File, such as de-veloper name, build date and the version of the JAR-File. This version defines the version of the TOE. This process is described in section 11.3 of [10].

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 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].

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 through enforced authentication data management.
- 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.
- 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: The HSM in FIPS mode enforces usage of smartcards. Thus all Administrators, Officers and Auditor must only use smartcards as authentication token between them and the HSM via CXI library.
- 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.
- 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. The IT environment provides reliable timestamps (NTP server).The connection between the management machine and the network components is protected by cryptographic transforms (e. g. SSH authorization and SSH transport protection).
- 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 approved cryptographic algorithms for authentication and signature generation/verification; approved key generation techniques and use validated cryptographic modules in the TOE environment.

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

5. Architectural Information

The TOE’s 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.
- Bootstrap: The subsystem Bootstrap interacts with the subsystems System and CA-Core, to ensure a secure initialization and boot process on the first initialization of the TOE.

These security functions are enforced by the following subsystems:

- **CA Core** (supports the TSFs SF2 and SF4). The CA-Core subsystem is responsible for CA-internal tasks such as key generation and issuing certificates. It has a defined Java-API for controlling the CA-Core (Java methods) and for storing CA-Core data (Output) via an adapter. The CA Core subsystem contains an interface to the HSM which is part of the protected TOE-Environment. The interface between CA-Core and HSM is Java Cryptography Extension (JCE). The CA Core subsystem contains an interace to the adapter which is part of the TOE environment. The interface between CA-Core and the adapter is a Java-API.
- **Audit** (supports the TSF SF1). The Audit subsystem protects audit messages against modification or deletion to ensure accountability of user actions. The Audit 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. For that the CA-Core sends the log messages to the Audit subsystem. The Audit subsystem then generates uniquely identifiable audit messages, so called audit records. The TOE triggers that a set of these chronologically ordered audit records (called audit trail) are periodically signed by means of a digital signature by the HSM, resulting in a so called protected audit trail. In order to protect audit messages against modification or deletion the Audit uses timestamps and audit trail sequence numbers. The Audit subsystem also triggers some cryptographic operations within the HSM to protect these messages. The TOE performs on every startup of the Audit an integrity check of the latest audit trail with HSM.
- **Bootstrap tool.** The Bootstrap tool (modelled as an own subsystem) is used to import or create a CA configuration and user certificates into the initial system without having to authenticate. Additionally the necessary keys for the encryption and signing of the audit trails are generated. The tool uses the external Java-API of the CA-Core subsystem to store the generated configurations. The bootstrap tool uses functions of the System subsystem to initialize the HSM and, if necessary, functions of the CA-Core subsystem

to initialize a new user CA and register it as a trust anchor in the HSM. Since the subsystem Bootstrap tool uses the functions and components of other subsystems for its security relevant operations, it does not directly support a TSF.

- **System** (supports the TSF SF1, SF2, SF3, SF4, SF5, SF6). The System subsystem is responsible for the initialization and provisioning of the interfaces of the various subsystems such as Audit or CA-Core. During the initialization, the system passes the implemented interfaces to fetch audit records and data from the adapter to the subsystems Audit and CA-Core. It also handles the checking of requests to the TOE interfaces, as well as forwarding the calls to the corresponding Audit or CA-Core subsystems. All calls or results of these calls are then logged accordingly by the system via the audit. Furthermore, after initialization of the HSM, the system makes the external interface to the HSM available to all other subsystems.

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 are 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,
- additional evaluator tests and
- 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 is installed on a standard PC fulfilling the requirements from chapter 1.2.3 of [6].

The following configuration is the configuration of the virtual machine and is consistent with the described one in Chapter 1.2.3 of [6]:

- 16 GB RAM
- Intel Core i7 @ 3.4 GHz
- 500 GB storage
- Network adapter
- power supply
- VGA graphics adapter

Utimaco HSM Emulator for Utimaco SE12 and Utimaco CP5

- CryptoServerCXI: Version 1.77
- CryptoServerAPI: Version 1.63
- bl_ver = 5.01.4.0 (Utimaco CP5)
- bl_ver = 5.01.4.4 (Utimaco SE12)

It is connected to two Utimaco HSMs and a personalised PinPad reader. This environment uses the RedHat 7 operating system. In the virtual environment the TOE is run on a virtual machine (VirtualBox) with virtual HSMs and a key file as a PIN pad substitute. The virtual environment is tested with all operating systems that are claimed in the ST [6]: Windows Server 2016, Windows Server 2019, RedHat Enterprise Linux (RHEL) 7 and RHEL 8.

Besides the requirements described in chapter 1.2.3 of [6], the test environment also needs to fulfil the security objectives for the environment. The TOE environment and the related test equipment for the tests are consistent with the described ones in [6] and [10]:

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 and the Bootstrapping. 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. 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 prove the correct implementation. All test cases were executed successfully and ended up with the expected result.

7.3. Independent Evaluator Testing

Overview

The independent testing was performed using the developer's test software environment. Specifically, the virtual lab environment using the RHEL 7 operating system was used. The configuration of the TOE being intended to be covered by the current evaluation was tested.

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

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

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

Test Configuration

The virtual test network used by the evaluators is only implemented with the VirtualBox with RedHat Enterprise Linux Version 7.7 and OpenJDK 11.0.6_10 and the HSMs simulators for both the Utimaco CP5 and Utimaco SE12 preinstalled.

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 a Test Suite: The Test Suite is not part of the TOE.
- In the 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.

Therefore the evaluators came to the conclusion that the TOE is platform-independent and therefore virtual testing of the TOE on only one platform is sufficient.

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

Repetition of developer’s test subset chosen

The evaluators chose to perform all developer tests on one operating system (RHEL 7). The tests performed by the developer have been assessed for all four platform and have been repeated by the evaluator on RHEL 7.

Independent test subset chosen

The independent test subset consists of eight individual tests. Each SFR-enforcing TSFI was tested at least once.

Evaluator test E1 covers the new method changeCertificateStateAndDelete() when it is called with a signature signed for a wrong Certificate. The test E2 covers that no security critical operations are allowed, when the TOE is in the AuditError State. Test E3 verifies that the TOE also starts up with only one HSM connected. The test E4 verifies that no bootstrapping can be performed on an already bootstrapped TOE. Evaluator test E5 verifies that the officer cannot fix the trail storage, but only the administrator. In evaluator test E7 the method fixTrailStorage with and without the parameter forceInit was tested. Evaluator test E8 covers the various certificate states and their transitions.

Verdict for the sub-activity

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

7.4. Vulnerability Analysis

Approach

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.

Firstly, the evaluator created a list of potential vulnerabilities based on the results gained while performing the vulnerability analysis in. This list merely consider 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 the ST [6], sections 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 in accordance to the attack potential, enhanced basic, which may be exploitable in the intended TOE's environment.

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.

Assessment

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 includes 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 conduct a focused search of ST, guidance and all other developer deliverables for the various evaluation aspects, to find potential vulnerabilities. Regarding the evaluation aspect IMP, the evaluators searched for common implementation flaws for Java-based applications. The advises 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 has been 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 configurations of the TOE: The TOE evaluated configuration is defined by the notation:

- secunet eID PKI Suite Certified CA Kernel
- Security Target [6]
- Manual [10]

- API Reference [11]
- Release Notes [12]

To identify the TOE as outlined in chapter 2.1 of the ST [6] the document [10] is providing sufficient information in chapter 11.

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 as follows:

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 1.2.3.3). The physical connections are:

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

JVM

The Certified CA Kernel 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 require one of the following JVM being present in its environment:

- Adopt JVM 11.0.6_10 with Open JDK 11.0.6_10
- Oracle JVM 11.0.6

Operating System

The Certified CA Kernel supports Windows Server 2016, Windows Server 2019, RHEL 7 and RHEL 8 operating systems. The operating system must be appropriately prepared for the operation of the TOE.

HSM

To be compliant with the CIMC PP [8] the certified Certified CA Kernel supports the following HSM

- Utimaco SafeGuard LAN V5 CryptoServers (SE12/52), certified according to FIPS 140-2 Level 3
- Utimaco SafeGuard LAN V5 CryptoServers CP5, certified in conformance to Pro-posed draft for Evaluation of ANSI-CC-PP-2016/05 in the Common Criteria scheme (EAL 4 + AVA_VAN.5).

The HSMs need the Utimaco CXI library in version 1.77 (delivered by Utimaco in form of the package SecurityServerEvaluation-V4.31.1.0). However, the CXI library is not part of the TOE.

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.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0960-2015, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the added HSM support (Utimaco CP5) and added API methods.

The evaluation has confirmed:

- PP Conformance: Certificate Issuing and Management Components Protection Profile Version 1.5, 11 August, 2011, Communications Security Establishment Canada, Document number: 383-6-3-CR [8]
- for the Functionality: PP conformant
  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 TOE does not include cryptographic mechanisms. Thus, no such mechanisms were part of the assessment.

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

AIS	Application Notes and Interpretations of the Scheme
API	Application Programming Interface
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
cPP	Collaborative Protection Profile
EAC CA	Extended Access Control Certification Authority
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HSM	Hardware Security 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

SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
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[8] https://www.bsi.bund.de/AIS

[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-1144-2021, Version 3.1.6, 18.12.2020, secunet eID PKI Suite Certified CA Kernel Version 2.0.3, secunet Security Networks AG

[7] Evaluation Technical Report, Version 1.2, 08.01.2021, 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 1.3.6, 18.12.2020, Konfigurationsliste ALC_CMS.4, cms_secunet+eID+PKI+Suite_V.1.3.6.pdf, secunet Security Networks AG (confidential document) and
Configuration list for the TOE, 06.11.2020, Liste aller source code-Dateien, dateiliste.txt, secunet Security Networks AG (confidential document)

[10] Guidance documentation for the TOE, Version 3.4.6, 18.12.2020, Handbuch (AGD_PRE.1 und AGD_OPE.1), Certified CA Kernel Manual.pdf, secunet Security Networks AG

[11] API Documentation - Commands, Parameters and Error Messages (JavaDoc), 18.12.2020, javadoc-cc.zip, secunet Security Networks AG

[12] Release Notes, Version 2.0.3, 23.10.2020, ReleaseNotes.pdf, secunet Security Networks AG

[8] specifically

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 38, Version 2, Reuse of evaluation results

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