Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0960-2015

for

secunet eID PKI Suite Certified CA Kernel, Version 1.0.0

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-0960-2015 (*)

Certificate Issuing and Management Component

secunet eID PKI Suite Certified CA Kernel
Version 1.0.0

SOGIS
Recognition Agreement

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

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 4

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

Bonn, 6 November 2015

For the Federal Office for Information Security

Bernd Kowalski
Head of Department

L.S.

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - 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.

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.

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

Contents

A. Certification

1. 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[2]
- BSI Certification and Approval Ordinance[3]
- BSI Schedule of Costs[4]
- 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]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [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]

2. 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.

2.1. European Recognition of ITSEC/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.

---

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

3 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

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

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

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). 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 new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. 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.sogisportal.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

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

2.2. 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 CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://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 nations listed above.

As the product certified has been accepted into the certification process before 08 September 2014, this certificate is recognized according to the rules of CCRA-2000, i.e. for all assurance components selected.

3. 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 1.0.0 has undergone the certification procedure at BSI.

The evaluation of the product secunet eID PKI Suite Certified CA Kernel, Version 1.0.0 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 9 October 2015. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] 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.

4. Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only 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 levels please refer to the excerpts from the criteria at the end of the Certification Report or in the CC itself.

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-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 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 6 November 2015 is valid until 5 November 2020. 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,
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,

[6] Information Technology Security Evaluation Facility

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.

5. Publication

The product secunet eID PKI Suite Certified CA Kernel, Version 1.0.0 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[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] secunet Security Networks AG
Kronprinzenstraße 30
45128 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 Version 1.0.0 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 secunet eID PKI Suite Certified CA Kernel supports Extended Access Control Certification Authorities (EAC CAs) according to the BSI Technical Guideline TR-03110 [11] and International Civil Aviation Organization CAs (ICAO CAs), which are X.509 CAs according to ITU-T X.509 [12]. For cryptographic operations, the secunet CA Kernel relies on a FIPS-2 Level 3 validated cryptographic module – a Hardware Security Module (HSM) which is not part of the TOE.

The CA-Server administrator integrates the secunet eID PKI Suite Certified CA Kernel into a TOE functional environment. He is defined as TOE end-user.

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 [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 subsystem 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. That is, the subsystem CACore logs amongst others every event and the appropriate event state, in the case that this event triggers a process of the CACore. If the audit trail is full the TOE will shut down.
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 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: Object identity, user identity and event type. 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 Hardware Security Module. 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. The Audit needs three different cryptographic keys to protect the audit trails. It needs one signature key (ASK), one

TOE Security Functionality	Addressed issue
	encryption key (AEK) and also one current symmetric trail record key (TRK). All these keys are generated within and stored on the HSM.
SF2 Management of the TSF	At the first startup of the TOE, the CACore has no configuration. Thus, the CACore must first be configured via the Java-API. The CACore 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 and the CACore triggers the generation of a new symmetric key within HSM. Then the CACore triggers HMAC protection of the configuration within the HSM. Finally the CACore stores the HMAC protected configuration via Java-API to the Adapter. (All data of Certified CA Kernel may be stored in or retrieved from a database via an Adapter.) If a configuration is needed during processing, the CACore loads all information via Java-API from the Adapter. Then the CACore triggers HMAC verification within the HSM. If HMAC verification fails the Audit generates an audit log record and the CACore does not further continue processing. If HMAC verification succeeds the CACore Job processing is continued.
SF3.1 Challenge Request and Response	In order to prevent replay attacks, the CACore triggers a challenge-response algorithm. In a first step, the external component must request a challenge via the Adapter from the CACore. The CACore then triggers generation of a challenge within the HSM. The CACore then stores the challenge with the user identification given in the request and sends the challenge back to the external component via the Adapter. Now the external component may request Job processing via the 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 the CACore starts a particular process it performs the following checks to ensure the integrity of the consigned Java method data: The CACore ● 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. The allowed roles are: Administrator, Auditor and Officer. 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 CACore does not start request processing.
SF4 Certificate and Certificate Status Management	The TOE triggers the generation of X.509 certificates and CRLs according to the standards X.509v3 [12] and RFC 5280 [13]. In addition to this, the TOE also generates CVC for EAC e-Passport infrastructure according to the BSI TR-03110 [11] 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 [13]).
SF4.1 Certificate Generation	In case of a certificate request, the CACore ● validates the certificate request against the loaded CAProfile,

TOE Security Functionality	Addressed issue
	● triggers signature verification of the certificate request within HSM, ● transforms the CAProfile and merges it with the certificate request into a certification template, ● triggers the signing of a 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 CACore ● merges the CRLProfile and the list of revoked certificates into the certificate revocation list template, ● triggers the 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 specified in Section 9.1 of [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. When a controlled resource is accessed, the CACore 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 [14] validated cryptographic module – a Hardware Security Module (HSM). All cryptographic operations (key generation, hashing, signing, verifying and key zeroizing) are performed within this validated cryptographic module. The HSM runs in FIPS mode. Here, FIPS mode means FIPS approved mode of operation according to [14]. 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 CACore. Component private keys are only stored on the HSM. The integrity and authenticity of public keys stored by the TOE in 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 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 in FIPS mode: ● Generate Key

TOE Security Functionality	Addressed issue
	● En/Decrypt Data ● Sign Data ● Verify Signature ● Compute Hash ● Agree/Handle shared 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], chapters 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, Version 1.0.0

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	**secunet_eID_PKI_Suite_CertifiedCAKernel-1_0_0.zip** (contains #2 to #6)	Version 1.0.0	Via Download or DVD/CD
2	SW	**CertifiedCAKernel.jar** SHA256 checksum: 82c1a41893944d4e18dca82d3f144de0b830c14e83cf64a641c7b52edb7b0192	Version 1.0.0	As part of #1
3	SW	**bootstrap.bat** SHA256 checksum: 7dbe04657b939d384c96bbc9af8337b8505acd69c51469dffce10bfa419b7d08	Version 1.0.0	As part of #1
4	DOC	**Manual Certified CA Kernel.pdf** [10] SHA256 checksum: 5ffd82d9e84212b60179437d347e5953b6f37ec6bd97642af80db68ddb432c9f	Version 1.03	As part of #1

No	Type	Identifier	Release	Form of Delivery
5	DOC	**Security Target Certified CA Kernel.pdf** [6] SHA256 checksum: d4e6088b749c2891846e2e25a813e7bdf398d7e02b64d9977048a68655584b07	Version 1.07	As part of #1
6	DOC	**ReleaseNotes.pdf** [15] SHA256 checksum: 1fc1813a0c464eda3933877ec47e8c636551de619a94f25adcd345c475d8ca10	Version 1.0	As part of #1

Table 2: Deliverables of the TOE

The software consists of two files which can be uniquely identified by their hash checksums given in the table above (#2 and #3). The version number of the TOE is 1.0.0.

The user is provided with guidance for TOE identification in [10] (#4 in the above table).

The TOE is delivered via the secunet download portal or personally delivered to the application developer on a CD/DVD. The project manager at secunet describes the integrity and authentication checks to the application developer by phone or personally.

The end-user can verify that the authenticity and integrity of the TOE has not been altered. First the signed zip file must be verified. Therefore the user uses the public verification RSA key delivered with the zip file (#1 in the above table), with the SHA256 fingerprint given to him by the developer. After a successful verification, the hash values of the binary parts of the TOE can be compared to the ones given in Table 2. This calculation can be done with any available SHA256 program.

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 public key certificates and determine certificate status and CA functionality to generate certificates and certificate status information as well as audit data generation according to example CIMC-3 (single component) of CIMC PP [8]. Specific details concerning the above mentioned security functionalities can be found in section 6 of the Security Target.

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.
- 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. (Validated is defined as FIPS 140-2 validated.). The cryptographic module is required to run in FIPS mode.

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. For cryptographic operations the secunet CA Kernel relies on a FIPS-2 Level 3 validated Hardware Security Module (HSM).

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

In the TOE design, 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 System, Audit, CACore and supports Bootstrap for the secure initialization.
- Audit (supports the TSF SF1): The subsystem Audit interacts with the subsystem System and provides message generation and protection of the Audit trails.
- CACore (supports the TSFs SF2 and SF4): The subsystems CACore 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

Figure 1 visualizes the TOE Design and its TSFIs in the TOE structure.

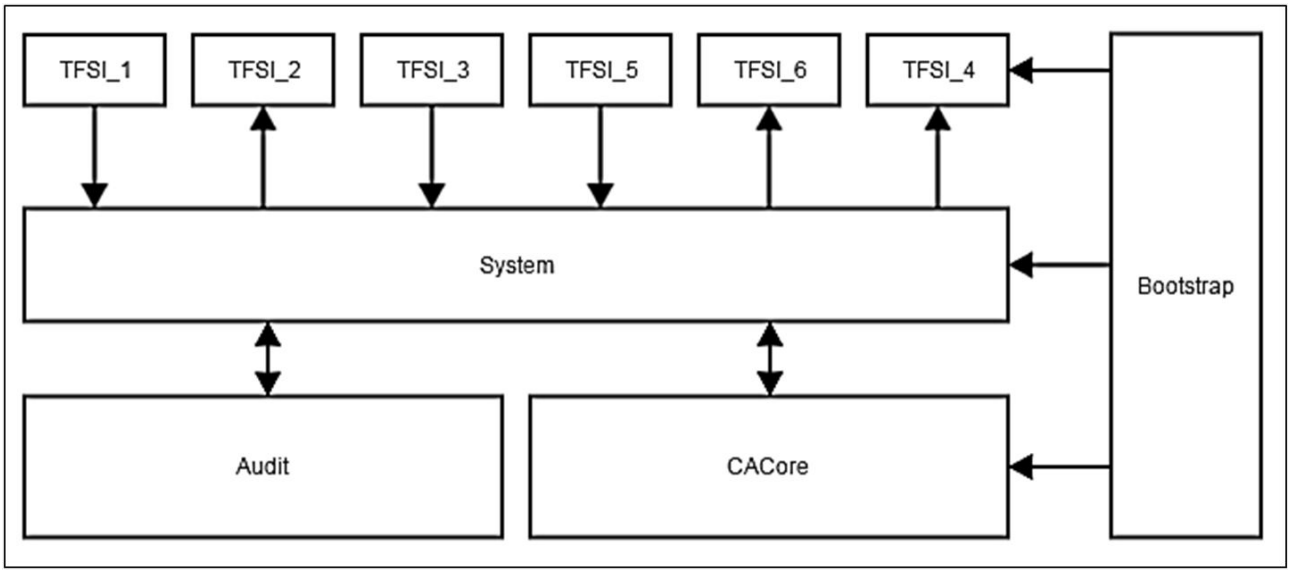

Figure 1: Visualization of TOE Design

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

The TOE test configuration is defined by “secunet eID PKI Suite Certified CA Kernel” with the hash values for the two binary parts of the TOE as given in table 2 above. Therefore the evaluated configuration and the configuration tested during evaluation were confirmed to be the same.

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
- Additional evaluator tests
- Vulnerability analysis

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

The achieved test results corresponded to the expected test results.

7.1. Functional Testing

TOE Test Configuration

The TOE was tested in the secunet testing environment. The TOE was installed on a standard PC fulfilling the requirements from chapter 1.2.3 of [6]. It was connected to the Utimaco HSM and a personalised PinPad reader. 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 evaluators compared the requirements for the operational environment with the actual testing environment of the developer. 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 divided into those of the CACore, 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. The tests can be run and the framework 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 was logged.

Testing Results

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

7.2. Independent Evaluator Tests

Overview

The independent testing was performed using the developer's testing environment. 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.

Test Configuration

The TOE was tested in the secunet testing environment. The TOE is installed on a standard PC fulfilling the requirements from chapter 1.2.3 of [6]. It is connected to the Utimaco HSM and a personalised PinPad reader. 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 evaluators compared the requirements for the operational environment with the actual testing environment of the developer. The TOE environment and the related test equipment for the tests are consistent with the described ones in [6] and [10].

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

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

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

Utimaco HSM

- Utimaco Package Version 3.11.0 (contains the CXI library)

Utimaco HSM Emulator

- CryptoServerCXI: Version 1.61
- CryptoServerAPI: Version 1.49
- bl_ver = 3.00.3.0

The configuration was verified by the evaluator during the ATE workshop.

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

Subset size chosen

The independent test subset consists of eight individual tests. Each TSFI was tested at least once. The tests cover especially the quality of imported certificates using different configurations using one or two HSMs. Security critical operations during states and the bootstrapping mechanism was part of the tests. Tests to ensure the correct usage of parameters during audit functionality in different states were also part of the subset.

Developer's test subset repeated

From the developer tests a subset of six tests was generated. These tests were chosen because they cover all TSFIs of the TOE. In all test cases the expected result was met.

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

7.3. Vulnerability Analysis

The evaluators 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 the 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 considering the current TOE type,TOE specific technology, and TOE specific implementation.

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.

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.

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.

Due to the fact that there are no potential vulnerabilities identified that are not analysed in vulnerability analysis of the evaluator there was no further penetration testing done by the evaluator.

The test results fulfil the requirements of AVA_VAN.3.

8. Evaluated Configuration

This certification covers only one configuration of the TOE that is defined in chapter 1.2.3 and chapter 2.1 of the Security Target [6] and in chapter 12 of the guidance documentation [10].

The Certified CA Kernel supports Windows Server 2012 R2 operating system. The operating system must be appropriately prepared for the operation of Certified CA Kernel. It is sufficient if the operating system was installed in the basic configuration. Particularly, the server does not need any additional services such as print servers or web servers. In addition to the base installation, the package 'Oracle Java SE 8u45' must be installed.

The evaluated configuration only supports HSMs. The TOE evaluated configuration comprises the Utimaco HSM package version 3.11.0, which also includes the CXI library. 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.

The evaluation has confirmed:

- PP Conformance: Certificate Issuing and Management Components Protection Profile Version 1.5, 11 August, 2011 [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.

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. Definitions

12.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BAT	Batch File
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 CA
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

12.2. 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.

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012, http://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-0960-2015, Version 1.07, 08.10.2015, secunet eID PKI Suite Certified CA Kernel Version 1.0.0 Security Target, secunet Security Networks AG

[7] Evaluation Technical Report, Version 1.3, 09.10.2015, Evaluation Technical Report (ETR) – Summary, Lab-Name, (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 0.92, 16.07.2015, Konfigurationsliste ALC_CMS.4 (confidential document)

[10] Guidance documentation for the TOE, Version 1.03, 21.08.2015, Handbuch (AGD_PRE.1 und AGD_OPE.1)

[11] TR-03110, BSI, Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents, Part 1-3, Version 2.10, 20.03.2012, https://www.bsi.de

[12] ITU-T X.509, Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, http://www.itu.int

[13] RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008, http://tools.ietf.org/html/rfc5280

[14] FIPS140-2 Federal Information Processing Standards Publication, FIPS PUB 140-2, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, NIST, 12.03.2002, http://www.nist.gov

[15] Release Notes, secunet eID PKI Suite Certified CA Kernel Version 1.0.0, Version 1.0, 10.07.2015

[8] specifically

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

C. Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model

Assurance Class	Assurance Components
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one

component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Evaluation assurance level 1 (EAL 1) - functionally tested (chapter 8.3)

“Objectives

EAL 1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL 1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL 1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL 1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL 2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering."

Evaluation assurance level 4 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs."

Evaluation assurance level 5 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques."

Evaluation assurance level 6 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL 6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs."

Evaluation assurance level 7 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.