Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0994-2019

for

SecDocs Security Komponenten, Version 2.4

from

OpenLimit SignCubes AG

sponsored by

Fujitsu Technology Solutions GmbH

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-0994-2019 (*)

SecDocs Security Komponenten, Version 2.4

from	OpenLimit SignCubes AG
sponsored by	Fujitsu Technology Solutions GmbH
PP Conformance:	Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Long-Term Preservation of Electronic Documents, Version 1.2, 28 March 2014, BSI-CC-PP-0049-2014, Bundesamt für Sicherheit in der Informationstechnik
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.1

SOGIS
Recognition Agreement

Common Criteria

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

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

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

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

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

Bonn, 19 September 2019

For the Federal Office for Information Security

Bernd Kowalski
Head of Division

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.

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

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

2 Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

3 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

- 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.sogisportal.eu.

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

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

3.2. International Recognition of CC – Certificates (CCRA)

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

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

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

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

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

4. Performance of Evaluation and Certification

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

The product SecDocs Security Komponenten, Version 2.4 has undergone the certification procedure at BSI.

The evaluation of the product SecDocs Security Komponenten, Version 2.4 was conducted by T-Systems International GmbH. The evaluation was completed on 12 September 2019. T-Systems International GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the applicant is: OpenLimit SignCubes AG.

The sponsor is: Fujitsu Technology Solutions GmbH.

The product was developed by: OpenLimit SignCubes 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 19 September 2019 is valid until 18. September 2024 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

[5] Information Technology Security Evaluation Facility

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 SecDocs Security Komponenten, Version 2.4 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] OpenLimit SignCubes AG
Zuger Straße 76 B
CH 6341 Baar
Switzerland

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 SecDocs Security Komponenten, Version 2.4. The TOE is a software product providing amongst others the core of an ArchiSafe compliant archive middleware and is providing security functionality conformant to the protection profile for an ArchiSafe compliant middleware [8]. The TOE is part of the software product “SecDocs Version 3.0” and is delivered together with additional software.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Long-Term Preservation of Electronic Documents, Version 1.2, 28 March 2014, BSI-CC-PP-0049-2014, Bundesamt für Sicherheit in der Informationstechnik [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.1.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.2. 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
SF 1	Secure Client TOE Access: Preventing the access to the storage systems from unknown client applications by reliable identification and authentication of these external entities.
SF 2	Data Object Verification: Preventing the storage of submission information packages (SIP) which in whole or in part cannot be verified successfully corresponding to the rules deposited in the TOE in order to guarantee interoperability between client applications and storage systems.
SF 3	Secure Storage Unit Access: Forwarding of successfully verified SIP’s to the dedicated storage systems only or another trusted application which in turn forwards the SIP to the dedicated storage systems only.
SF 4	Invalid Archival Information Package Erasure Prevention: Preventing the deletion of AIP’s before the expiry of their retention time without a justification.
SF 5	Retrieval and delivery of AIP from the dedicated storage system (to the CS) only.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7[7].

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.2. 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 3.3, 3.4 and 3.5.

[7] The security functionality SF3 and SF5 are both addressed in the ST [6] in chapter 7.3 named ‘SF 3’. The TOE is implemented in such a way, that storing and retrieval to and from the SU use both the same security mechanisms.

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:

SecDocs Security Komponenten, Version 2.4

The following table outlines the TOE deliverables:

No	Type	Identifier, SHA256 Hash Value	Release	Form of Delivery
1	SW	Archive file SecDocs_Security_Components_v.2.4.zip SHA256: eef9a24b2c31330624adcd5a8cd83a7a145469f59e1301302fb4cb22f76271a4	v2.4	Software downloaded from login-protected servers of the developer
2	SW	Archive file MigSafeOverSign-V2.4.zip containing the TOE's JAR files and the JavaDoc API documentation SHA256: 639560fe28502429b6dde3d45ffe450c972f392c992167df48142d09eeca5001	v2.4	Part of the archive file no. 1: SecDocs_Security_Components_v.2.4.zip
3	DOC	Integrator's manual MSOS_Integratorhandbuch_DE.pdf SHA256: 3ac72f1238a3905a4de9b761e064a8d7a150aa211b4a389fe66aeaa63bc9cd26	05.06.2019	Part of the archive file no. 1: SecDocs_Security_Components_v.2.4.zip
4	DOC	Administrator's manual MSOS_Admininstratorhandbuch_DE.pdf SHA256: 0f26f5732266ac8fbd974676e9cd860998aaa873097303da5d1e41d77ae6952d	05.06.2019	Part of the archive file no. 1: SecDocs_Security_Components_v.2.4.zip
5	DOC	TOE's functional specification ADV_FSP-MigSafe-OverSign_2.4_2019-08-06.pdf SHA256: 8b8aa1e4ee9f6ac305da8000d5ec927b773a581dbcf1cc5e046942646dd45237	06.08.2019	Part of the archive file no. 1: SecDocs_Security_Components_v.2.4.zip

No	Type	Identifier, SHA256 Hash Value	Release	Form of Delivery
6	DOC	Administrator's manual of the non-TOE component OpenLimit Middleware Version 3 Server, Produktversion 1.6 Administratorhandbuch_V3_Server_v.1.35.pdf SHA256: 02ecf718739c531f75cfb865b3b6ad82a3a21d42fb92b1234c39a3cb74596ad8	13.02.2018	Part of the archive file no. 1: SecDocs_Security_Components_v.2.4.zip
7[8]	SW	Archive file MigSafeOverSign-V2.4.563_13022_SecureInterfaceTools.zip containing examples for the TOE integration	v2.4	Part of the archive file no. 1: SecDocs_Security_Components_v.2.4.zip

Table 2: Deliverables of the TOE

The TOE is delivered to the customer by the OpenLimit SignCubes AG using the following delivery procedure: The TOE is downloaded from the partner portal under the address https://partner.openlimit.com/svn/secdocs via an HTTPS secured connection. A login to this portal is required for downloading the software. The username and the initial password are transferred to the customer through an encrypted e-mail.

The TOE documentation (items 3 to 6 of table 2) is delivered in electronic form by the developer as part of the archive file that contains the TOE.

The TOE can be identified using the cryptographic hash value of the archive file "SecDocs_Security_Components_v.2.4.zip": eef9a24b2c31330624adcd5a8cd83a7a145469f59e1301302fb4cb22f76271a4

Note that by this it is ensured that both the TOE software and the TOE documentation are valid. For additional unique identification, the SHA256 checksum of all files delivered within the archive file are given in table 2 above.

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 security policy enforced is defined by the selected set of SFRs and implemented by the TOE. The TOE implements logical security functionality in order to enable the long-term preservation of electronic documents by implementing the ArchiSafe concept developed by the Physikalisch-Technische Bundesanstalt (PTB). Hence, the TOE enforces decoupling and access control storage systems used for the long-term preservation of (cryptographically signed) electronic documents. The TOE also enforces the provisioning of a justification, if archived data shall be deleted before its retention time.

Therefore the TOEs policy is to protect the data flow between third party applications (such as document management systems) and storage solutions. Besides, the TOE prevents access to storage systems from unknown client applications through identification and authentication and manages operations that client systems are allowed to execute on archived data objects. Specific details concerning the above mentioned security policies can be found in Section 6.1 of the Security Target [6].

[8] The TOE consists of the artefacts 1 to 6 listed in table 2. They are combined in the single archive file artefact 1. Artefact 7 contains examples for the TOE integration and is delivered together with the TOE as part of artefact 1, it is however not part of the evaluated configuration.

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.AUTHENT: The client software applications (CS), the storage unit (SU), and any trustworthy special applications which are authorized by the IT-Environment for using the TOE or to be used by the TOE, have to be configured in such a way that they identify and authenticate the TOE before any data transfer.

  The integrator has to refer to section 5.4.4 of [10].

- OE.CONFIGURATION: The TOE has to be securely configured and all data required for the configuration of the TOE must secure and reliable transported to and installed on the machine which runs the TOE.

  The administrator has to refer to section 3.1 of [11].

- OE.EVIDENCEDATA: The generation, storage, management and renewal of evidence data for proving the unmodified existence of archival information packages at a certain time shall be provided by trustworthy special applications in a secure non-TOE environment.

  The integrator has to refer to section 5.4.4 of [10].
  The administrator has to refer to section 3.1 of [11].

- OE.RULES: Rules defined for operating on archive objects and archive requests by the TOE must not introduce any security risk.

  The integrator has to refer to section 4.1 of [10].

- OE.PHYSPROT: The machine on which the TOE runs must be protected against unauthorized physical access and modification.

  The integrator has to refer to section 4.1 of [10].
  The administrator has to refer to section 3.1 of [11].

- OE.COMMUNICATION: The communication inter-connections between the TOE and all non-TOE components and systems, have to be protected by the environment – by physical or logical security measures – against disclosure as appropriate regarding the need for information disclosure of the clients. The communication interconnections between the TOE and all non-TOE components and systems must be protected by the environment – by physical or logical security measures – against threats (e. g. disclosure) which may compromise the security objectives of the ST.

  The integrator has to refer to section 4.1 of [10].
  The administrator has to refer to section 3.1 of [11].

- OE.NO_BYPASS: The TOE must be integrated in the IT environment in such a way that all storage access by the CS cannot bypass the TOE, if it is mandated or required by policies of the organization which uses the TOE.

  The integrator has to refer to section 4.1 of [10].

- OE.ADMIN: The administrators of the TOE, of the crypto provider cryptographic or other trustworthy 3rd party components connected to the TOE, of the storage system, the underlying systems, and of the communication connections (e.g. the LAN) must not be

careless, wilfully negligent, or hostile, and will follow and abide the instructions provided by the administrator's guidance. They shall be well trained to securely and trustworthy administer all aspects of TOE operation as well as all other involved processes or operations in accordance with the guidance. The administrators shall protect their credentials used for authentication. Credentials must not be disclosed to other individual.

The integrator has to refer to section 4.1 of [10].
The administrator has to refer to section 3.1 of [11].

- OE.SERVER: The machine on which the TOE, systems and application run must be free from malware and viruses. Systems and applications running on the server must be securely installed. An unauthorized access to functions, processes and data of the TOE must not be possible.

  The administrator has to refer to section 3.1 of [11].

- OE.STORAGE: The dedicated SU must provide a reliable, secure and available storage of archival information packages (AIP), even for long-terms.

  The integrator has to refer to section 5.5 of [10].

- OE.TIMESTAMP: The environment shall be able to provide reliable time-stamps to the TOE.

  The integrator has to refer to section 4.1 of [10].

- OE.TOKEN: The environment, e. g. the SU or another non-TOE part of the middleware, has to provide a reliably generated unique archive object identifier (AOID) for any successfully archived submission information package.

  The integrator has to refer to section 4.1 of [10].

- OE.TRUSTAPP: The archive requesting CS has to provide sufficient trust to be assumed as secure and has at least to provide reliable measures regarding the authentication and access control of its (human) users.

  The integrator has to refer to section 4.1 and 4.3 of [10].

- OE.TRUSTCRYPTO: Only trustworthy cryptographic components are allowed to be used. The cryptographic components must not send any security relevant and confidential data to any external entity and have to reliably protect all security relevant and confidential data from disclosure by an external entity.

  The integrator has to refer to section 4.1 of [10].

Details can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

The TOE mainly decouples the data flow (i.e. the flow of archive objects) between third party applications, such as document management systems, and the long-term storage solutions. The architecture of the complete system is shown in Figure 1.

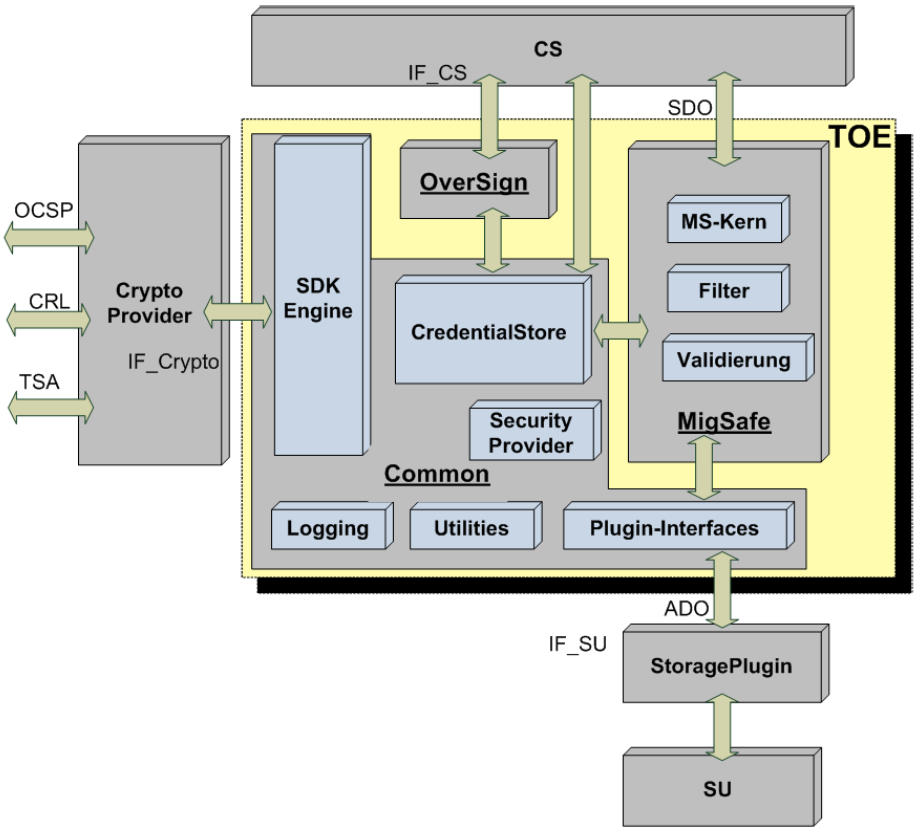

Figure 1: Architecture of the TOE

The TOE has three external interfaces:

- IF_CS: This represents the interface between the TOE and an external client system (CS) which submits and receives the (cryptographically signed) information to be preserved.
- IF_SU: This represents the interface between the TOE and an external storage unit (SU) which preserves the (cryptographically signed) information.
- IF_Crypto: This represents the interface between the TOE and an external crypto provider which is used for cryptographic operations on the (cryptographically signed) information to be preserved.

Internally, the TOE consists of three subsystems as shown in the following table:

Subsystem	Description
Common	● Functionalities of accessing an external crypto provider component and an evidence preservation component (module SecurityProvider) ● Functionalities of accessing an external crypto provider component (module SecurityProvider) ● Functionalities of accessing an external audit/logging plugin (module Plugin-Interfaces) ● Functionalities of accessing an external storage plug-in (module Plugin-Interfaces) ● Functionalities of maintaining a volatile user database (module CredentialStore) ● Functionalities of logging of the TOE's executions (module Logging) ● Generic functionalities like converting data types or usage of certificates (module Utilities)
MigSafe	● Functionalities of defining the interfaces of the CS to the subsystem MigSafe of the TOE (module MS-Kern) ● Functionalities of accessing the long-term-storage via the module Plugin-Interfaces of the subsystem Common (module MS-Kern) ● Functionalities of validating data objects against XML schemes (module Validierung) ● Functionalities of filtering XML documents (module Filter)
OverSign	● Functionalities of requesting and checking of evidence records ● Functionalities of generating hash values ● Functionalities of checking time stamps

Table 3: Subsystems of the TOE

6. Documentation

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

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

7. IT Product Testing

7.1. Developer Testing

The developer considered the TOE environment as defined in the Security Target [6]. The developer tests cover all three subsystems Common, MigSafe, and OverSign, as described in chapter 5.

Moreover, aspects of the security architecture of the TOE are also covered by tests conducted by the developer. Each test is implemented as an automatic test based on the JUnit test framework and is executed on the operation systems Red Hat Enterprise Linux Server (RHEL) 6.5 64 bit, Red Hat Enterprise Linux Server (RHEL) 7.0 64 bit, and SUSE Linux Enterprise Server 11 SP 3 64 bit, together with the OpenJDK version 8u202, and the CryptoProvider component "OpenLimit-Middleware-Version-3-Server-

1.6.2.3.2017062801.x86_64 mit OpenLimit-Middleware-Version-3-Server_AlgCats-1.6.2.5”. All tests were executed by the JUnit framework without further user action.

The test documentation consists of a test coverage and depth of testing analysis, a test plan, test specifications for each of the security functionalities (SF1, SF2, SF3, and SF4), and test result logs. The particular test specifications show:

- Goal of testing
- Testing steps
- Test description
- Test preconditions
- Test conduction
- Expected results

The test result logs show that the tests identified in the test coverage and depth of testing analysis have been executed as expected by the developer.

7.2. Independent Evaluator Testing

Overview:

The independent testing was partially performed using the developer’s testing environment, partially using the test environment of the evaluation facility. The developer’s testing environment implements the external infrastructure required to operate the TOE with the evaluator’s setup.

Since the TOE has only one configuration, all configurations of the TOE being intended to be covered by the current evaluation were tested.

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

Independent testing approach:

The TOE was independently tested with respect to three subject areas:

- The usage of TLS connections to external components, which the TOE uses to exchange archive data for storing or loading, and the usage of random data for crypto operations,
- the correct usage of XML input data which the TOE uses for submission information packages and
- the correct authentication of client systems through usage of contexts for calling operations of credential stores.

TOE test configurations:

No special configuration is made. The TOE has only one single configuration, and the TOE is always in this default configuration.

The TOE under test is “SecDocs Security Komponenten, Version 2.4” consisting of the following components:

- CredentialStore.zip, SHA256: cdf2be3505229716e4305bd01db43e107d2e14cbcf4161ee67baee4a064a724a

- CredentialStore.jar from CredentialStore.zip, SHA256: 4b1c4271c3d002ba4c11930e2222d2469472fd6b989f3f24ff5f30d4e8f8c888
- MigSafeLibrary.jar, SHA256: 794e232c25735c6666f7a73605cb03f09e12832dfd949c28fcc09012e83a4dcf
- OverSignLibrary.jar, SHA256: a1568d5ce04535cc27c6e3d355d3345666935f538f201f1b501322a38e731083
- XMLFilter.jar, SHA256: 8009712e6387052d3f9d2b22263b2ab115a22c54b84e0c6e48021150de8b4f11
- bcprov-jdk15on-160.jar, SHA256: d65bf7e1a3dae9a8ae2ad9cb64ef443ea089b1ad930dca999f70bbab56d9f349
- jsse.jar from CredentialStore.zip, SHA256: ff0d233737cfb9fd19dc4de16a9c391a789e1256847b64d39347592a6606a9ea
- sunec.jar from CredentialStore.zip, SHA256: b2231d1f6bccebd58547707361bfc19f783da54df5da263d327eca39e2dd5db6
- sunjce_provider.jar from CredentialStore.zip, SHA256: 1ccb46312b062f16715fe2807a9a0e51478b558b0797d0d6b9e021b0e352f8da

The operation system used was “CentOS 7 64 bit” in combination with the OpenJDK versions “1.8.0 build 212-b04”[9], “Junit 4.12” and the CryptoProvider component “OpenLimit-Middleware-Version-3-Server-1.6.2.3.2017062801.x86_64 mit OpenLimit-Middleware-Version-3-Server_AlgCats-1.6.2.5”.

Independent test subset:

The TSFIs tested by independent evaluator tests are IF_CS, IF_Crypto, and IF_SU (see chapter 5). This includes all major interface functionalities like communication with the client software application, the crypto provider, the storage unit and other trustworthy application (e.g. the Evidence Preservation Component) as well as input data processing. These interfaces are most critical for the security that the TOE provides.

Developer’s test subset repeated:

The evaluators repeated developer tests for four important subject areas:

- The correct CMAC implementation,
- the repudiation of non-authenticated archive operations,
- the repudiation of invalid certificates, and
- the correct usage of embedded signatures in PDF documents.

All those tests cover critical security functionalities of the TOE and are developer-coded implementations.

SFRs tested:

The SFRs tested by the subset of the developer tests repeated by the evaluators cover: FAU_GEN.1, FCS_CKM.1/TLS, FCS_COP.1/TLS, FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1, FIA_UAU.2, FIA_UID.2, FMT_MSA.1 (Rules), FMT_MSA.3 (Access),

[9] The developer provided a VM that uses OpenJDK 1.8.0 212-b04, instead of version 8u202 as listed in sec. 1.3.3 of the ST [6]. The documented tests were conducted under the provided JDK version 1.8.0 212-b04 but later were repeated by the evaluators under JDK version 8u202. The evaluators can confirm that for both JDK versions the test results are the same.

FMT_MSA.3 (Rules), FMT_SMR.1,FTP_ITC.1 (CRYPTO), FTP_ITC.1 (CS), and FTP_ITC.1 (TAPP).

Verdict for the sub-activity:

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

7.3. Penetration Testing

Overview:

The penetration testing was partially performed using the developer's testing environment, partially using the test environment of the evaluation facility.

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

The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential Enhanced-Basic was actually successful.

Penetration testing approach:

The evaluator examined the developer document [10] to find relevant information about how to bring the TOE in a proper and known state. He then searched for potential vulnerabilities through CVE entries based on the design and architecture documentation. In addition to that the evaluator searched for potential vulnerabilities for the TOE whilst evaluating the developer contributions for the single evaluation aspects in the context of the assurance classes ADV, AGD and ATE. The evaluator then derived attack scenarios which cover all potential vulnerabilities. For these scenarios the evaluator created penetration tests, so that every attack scenario is tested by at least one relevant penetration test.

TOE test configurations:

No special configuration is made. The TOE has only one single configuration, and the TOE is always this default configuration.

The TOE under test is "SecDocs Security Komponenten, Version 2.4" consisting of the components, as described in chapter 7.2:

The operation system used was "CentOS 7 64 bit" in combination with the OpenJDK version "1.8.0 build 212-b04"[10], "Junit 4.12" and the CryptoProvider component "Open-Limit-Middleware-Version-3-Server-1.6.2.3.2017062801.x86_64 mit OpenLimit-Middleware-Version-3-Server_AlgCats-1.6.2.5".

Attack scenarios having been tested:

- AS.1: The TOE receives manipulated CMAC values at its interface IF_CS in order to circumvent the authentication.
- AS.2: The TOE receives malformed certificates values at its interface IF_SU in order to circumvent the authentication.

[10] The developer provided a VM that uses OpenJDK 1.8.0 212-b04, instead of version 8u202 as listed in sec. 1.3.3 of the ST [6]. The documented tests were conducted under the provided JDK version 1.8.0 212-b04 but later were repeated by the evaluators under JDK version 8u202. The evaluators can confirm that for both JDK versions the test results are the same.

- AS.3: The TOE receives malformed XML values to parse input at IF_CS in order to exploit the XML parser.

SFRs penetration tested:

- FCS_CKM.1/AUTH tested through AS.1,
- FCS_COP.1/AUTH tested through AS.1,
- FDP_ACC.1 tested through AS.1,
- FDP_ACF.1 tested through AS.1,
- FIA_UAU.2 tested through AS.1,
- FIA_UID.2 tested through AS.1,
- FAU_GEN.1 tested through AS.1,
- FCS_COP.1/SIG tested through AS.2,
- FCS_COP.1/HASH tested through AS.2,
- FTP_ITC.1 (STORAGE) tested through AS.2,
- FMT_MSA.1 (Access) tested through AS.3,
- FMT_MSA.1 (Rules) tested through AS.3.

The remaining SFRs were analysed, but not penetration tested due to non-exploitability of the related attack scenarios in the TOE's operational environment also including an attacker with an Enhanced-Basic attack potential.

Verdict for the sub-activity:

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential Enhanced-Basic was actually successful in the TOE's operational environment as defined in the ST [6] provided that all required measures are applied.

8. Evaluated Configuration

This certification covers the following configurations of the TOE: The TOE "SecDocs Security Komponenten" is only available in one evaluated configuration comprising the versions of the software components as detailed in table 2. The versions of the software components can be identified through the instructions given in chapter 3 of "Administratorhandbuch", [11].

The TOE offers a legacy mode which does not protect the connection between the TOE and an external CryptoProvider component with TLS. This legacy mode is not part of the evaluated configuration and therefore must not be used in order to be compliant to this evaluation. The user has to follow the guidelines in section 3.1 of "Administratorhandbuch", [11] to operate the TOE in its evaluated secure mode.

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.

For RNG assessment the scheme interpretations AIS 20 and AIS 31 were used (see [4]).

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.1 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Long-Term Preservation of Electronic Documents, Version 1.2, 28 March 2014, BSI-CC-PP-0049-2014, Bundesamt für Sicherheit in der Informationstechnik [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.1

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

9.2. Results of cryptographic assessment

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

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

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Authenticity	ECDSA	TR-03111	256	yes	FCS_COP.1/SIG: identification and authentication of SU,

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
						CS, and crypto provider
2	Integrity	SHA256	FIPS 180-4	-	-	FCS_COP.1/HASH: protection of communication with CS, crypto provider, and SU against modification
3	Confidentiality, Integrity	TLS v.1.2 with cipher suite TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	RFC 5246, RFC 5289	128	yes	FCS_COP.1/TLS
4	Authenticity, Integrity	AES-CMAC	RFC 4493, NIST SP 800-38D	128	yes	FCS_COP.1/AUTH
5	Key Agreement	ECKA-EG with X9.63 KDF	TR-03116-3, TR-03111, FIPS 180-4	128	yes	Key Generation for FCS_COP.1/AUTH
6	Confidentiality, Integrity	FTP_ITC.1 (CRYPTO): Trusted communication channel between TOE and crypto provider using FCS_COP.1/TLS				
7	Confidentiality, Integrity	FTP_ITC.1 (CS): Trusted communication channel between TOE and CS using FCS_COP.1/AUTH				
8	Confidentiality, Integrity	FTP_ITC.1 (STORAGE): Trusted communication channel between TOE and SU using FCS_COP.1/AUTH				
9	Confidentiality, Integrity	FTP_ITC.1 (TAPP): Trusted communication channel between TOE and TAPP using FCS_COP.1/AUTH				
10	Random Number Generator	NPTRNG	AIS 20/31	-	-	FCS_RNG.1: DRG.2 for TOE identity generation

Table 4: TOE cryptographic functionality

10. Obligations and Notes for the Usage of the TOE

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

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

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

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

In addition, the following aspects need to be fulfilled when using the TOE:

- The TOE offers a legacy mode which is not part of the evaluated configuration – see chapter 8 – and therefore must not be used in order to be compliant to the certified configuration.
- For being used, the TOE has to been integrated into an ArchiSafe compliant archive middleware by the TOE integrator. Therefore, the TOE needs further parts of the ArchiSafe architecture being supplied by the TOE integrator: an implementation of a Client Software Application (CS), of the Crypto Provider Component, of the Evidence Preservation Component and of a so-called Storage Plugin as a trustworthy application interfacing with the long-term storage system (SU). The TOE can only been run in its integrated form. The software product “SecDocs v.3.0” offers such an integrated form of the TOE. For more information see the ST [6] and the Integrator’s Manual [11].

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

ADV CC Evaluation Class: Development

AGD CC Evaluation Class: Guidance Documentation

AIP Archival information package

AIS Application Notes and Interpretations of the Scheme

AOID Archive Object Identifier

ATE CC Evaluation Class: Tests

AVA CC Evaluation Class: Vulnerability assessment

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

BSIG BSI-Gesetz / Act on the Federal Office for Information Security

CCRA Common Criteria Recognition Arrangement

CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
CS	Client Software Application
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
OID	Object Identifier
PP	Protection Profile
PTB	Physikalisch-Technische Bundesanstalt
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SIP	Submission Information Package
ST	Security Target
SU	(Long-Term) Storage Unit
TAPP	**T**rustworthy Application
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 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012, 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[12] 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-0994-2019, Version 2.7, 23.08.2019, Security Target for SecDocs Security Komponenten, Version 2.4, OpenLimit SignCubes GmbH

[7] Evaluation Technical Report, Version 1.0, 03.09.2019, Evaluation Technical Report BSI-DSZ-CC-0994, T-Systems International GmbH, (confidential document)

[8] Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Long-Term Preservation of Electronic Documents, Version 1.2, 28 March 2014, BSI-CC-PP-0049-2014, Bundesamt für Sicherheit in der Informationstechnik

[9] Configuration list for the TOE, Version 7, 02.09.2019, EVG-CM-Liste (confidential document)

[10] Integrator’s manual, 05.06.2019, MSOS_Integratorhandbuch_DE.pdf

[11] Administrator’s manual, 05.06.2019, MSOS_Admininstratorhandbuch_DE.pdf

[12] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

[12] Administrator’s manual of the non-TOE component OpenLimit Middleware Version 3 Server, Produktversion 1.6, Version 1.35, 13.02.2018, Administratorhandbuch_V3_Server_v.1.35.pdf

[13] TOE’s functional specification, 06.08.2019, ADV_FSP-MigSafe-OverSign_2.4_2019-08-06.pdf

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 10.4
- 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 11
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 12 to 16
- 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