Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0685-2012

for

SecDocs Security Komponenten Version 1.0, build version 1.0.308_6236

from

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-0685-2012

SecDocs Security Komponenten Version 1.0
build version 1.0.308_6236

from	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 1.0, 31 October 2008, BSI-CC-PP-0049-2008
Functionality:	PP conformant Common Criteria Part 2 conformant
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.1

Common Criteria Recognition Arrangement

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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.

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, 10 September 2012

For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED

Bernd Kowalski
Head of Department

L.S.

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:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- 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 technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In Addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and

---

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 a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

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 United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

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

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. 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.

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 SecDocs Security Komponenten Version 1.0, build version 1.0.308_6236 has undergone the certification procedure at BSI.

The evaluation of the product SecDocs Security Komponenten Version 1.0, build version 1.0.308_6236 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 3 August 2012. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant is: Fujitsu Technology Solutions GmbH.

The product was developed by: OpenLimit SignCubes GmbH.

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.

[6] Information Technology Security Evaluation Facility

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification 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-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 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 SecDocs Security Komponenten Version 1.0, build version 1.0.308_6236 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] Fujitsu Technology Solutions GmbH
Mies-van-der-Rohe-Straße 8
80807 München

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 TOE is a software product providing the core of an ArchiSafe compliant archive middleware which acts as secure archive gateway. It provides the following general security functionalities:

- preventing the access to the archive from unknown client software application (CS) by reliable identification and authentication of these external entities,
- preventing the storage of invalid submission data objects (SDO) by reliable verification of the submission data object before forwarding them to the long-term storage unit (SU) or another trusted application which in turn forwards the SDO to the SU,
- forwarding of successfully checked SDOs to the dedicated SU only or another trusted application which in turn forwards the SDO to the dedicated SU only,
- preventing the erasure of archive data objects (ADOs) by any other CS than the CS which has also submitted this ADO and preventing the erasure of ADOs before expiry of their retention time without a justification.

The complete TOE reference is given by:

- SecDocs Security Komponenten Version 1.0, build version 1.0.308_6236.

The Security Target [6] is the basis for this certification. It is based on the certified Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Long-Term Preservation of Electronic Documents Version 1.0, 31 October 2008, BSI-CC-PP-0049-2008 [7].

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

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5.2. They are all selected from Common Criteria Part 2. Thus the TOE is CC Part 2 conformant.

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

TOE Security Functions	Addressed issue
SF 1	Secure Client TOE Access
SF 2	Data Object Verification
SF 3	Secure Storage Unit Access
SF 4	Invalid Archive Data Object Erasure Prevention

Table 1: TOE Security Functionalities

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

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 3.4 to 3.6.

This certification covers the following configurations of the TOE: TOE in build version 1.0.308_6236 and under consideration of Java SDK 1.6.0_24 in its 64 bit version (running on the operating systems RHEL 5.6/6.0 64bit). For details refer to chapter 8 of this report..

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 1.0, build version 1.0.308_6236.

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	(Static) SHA-256 hash value
1	SW	MigSafeLibrary.jar[8]	1.0.308_6236	29d3d2489039159090324 31f58b7f98e4af9c73e674fa7be2ec3067879725c7c
2	SW	OverSignLibrary.jar[9]		
3	SW	CredentialStore.jar[10]		
4	DOC	MigSafeOverSign-V1.0_Documentation.tgz		55cb8691150ae77b3171ab7d7c7149211da29678a4cdc9613b19d202fe871d68

Table 2: Deliverables of the TOE

The TOE is delivered as a piece of software with accompanying guidance [10]. The integrity of the TOE can be assured using cryptographic hash values. It consists of a set of jar files that have to be integrated in a software component by the TOE integrator. In other terms the TOE can only been used in its integrated form. The listed TOE libraries are specific for each TOE integrator. For checking the TOE integrity, at first the integrity of the TOE documentation archive has to be verified as following: The calculated SHA-256 hash value of the file “MigSafeOverSign-V1.0_Documentation.tgz” has to be equal to the value listed in table 2.

As second step, the so-called static SHA-256 hash value of the TOE’s libraries (aka. JAR archives) has to be verified according to the procedure described in the user documentation [10] as part of the verified TOE documentation archive: The calculated SHA-256 hash value of the TOE’s libraries has to be equal to the value listed in table 2.

[8] Integrator specific TOE library used in ATE.IND
21f96aae8865406f775fd49b6445fdd2692d3792906d33cd479ae2fc32a19cc6

[9] dfd66fdae8f9f59d29930cc043c5adb92defac1353d8c9a7ae2a05aaacd9ae66

[10] 65cc937e6516d43eecb77f49d8ea4f307ab3dc1ceb80f9439831db317562c9fa

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 controls the access to the archive permitting archive requests only from successfully authenticated CS. For a successfully identified and authenticated CS the TOE allows the following request types:

- Request for storing data objects in the storage
- Request for retrieving data objects from the storage
- Request for erasing data objects from the storage
- Request for retrieving evidence records
- Request for reading meta information

Thereby it prevents the storage of invalid data objects by reliable verification of the submitted data objects before forwarding them to the SU. In case of a successful verification the TOE securely passes the data objects to be archived to the SU. Moreover TOE prevents the erasure of ADOs by any other CS than the CS which has submitted this ADO and the erasure of ADOs before expiry of their retention time without a justification

4 Assumptions and Clarification of Scope

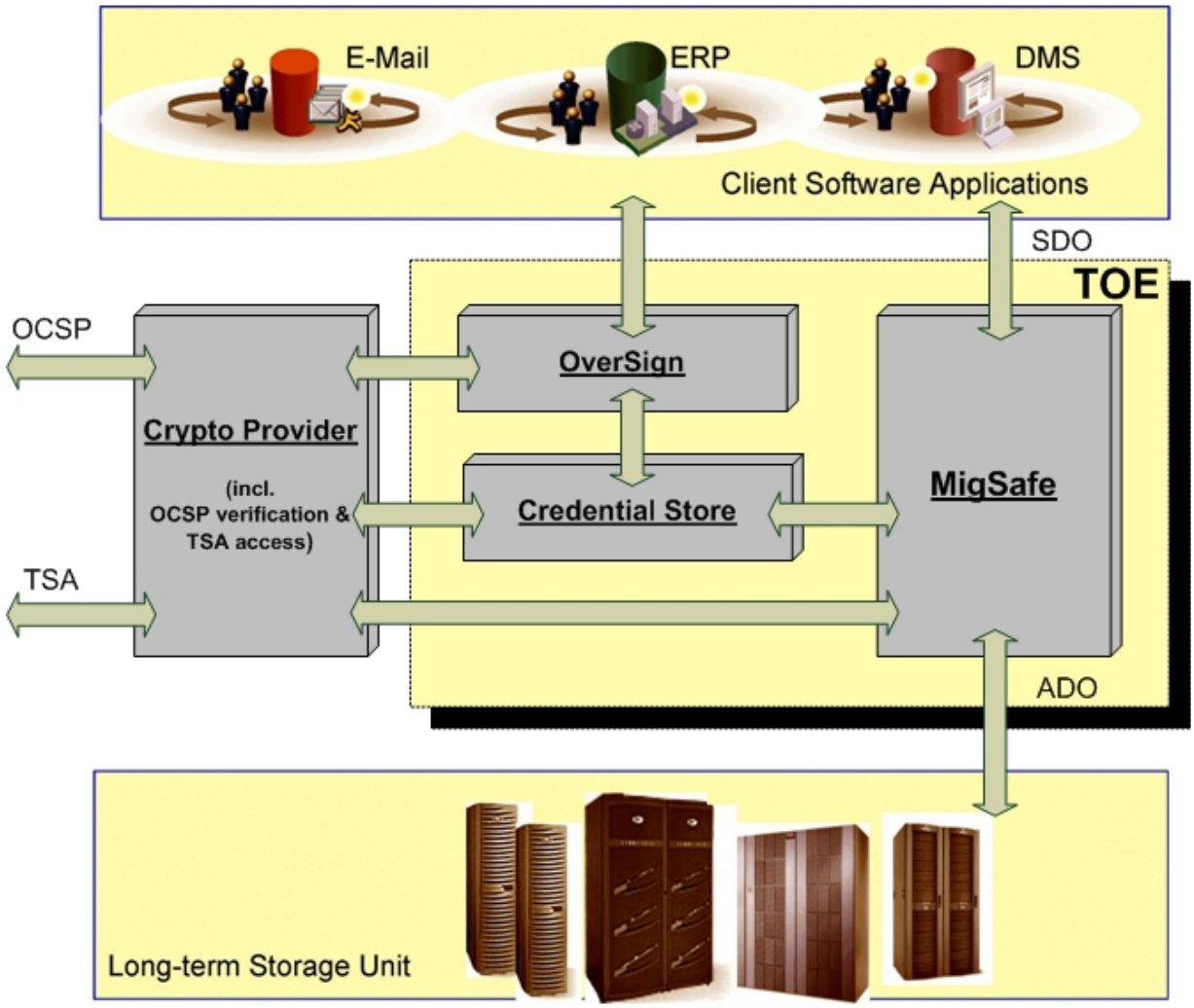
The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific Security Objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- Trained and trustworthy TOE administrators
- All CS authenticate the TOE before data transfer
- Protected communication interconnections
- Secure configuration of the TOE
- Trustworthy applications for evidence data
- Storage access by the CS must pass the TOE
- TOE runs on a physically protected server
- Secure server configuration
- Reliable and secure storage of data in the SU
- Reliable time-stamps provided by the environment
- Reliably generated unique archive object identifier (AOID) provided by the environment
- Secure CS with reliable authentication and access authorization of users
- Use of trustworthy cryptographic components

Details can be found in the Security Target [6], chapter 3.4.

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.



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

Subsystem	Description
Common (including Credential Store)	The subsystem “Common” includes • functionalities to access the crypto provider component (module "SDKEngine"), • definitions of the interfaces to the storage plugin and the audit and logging interfaces (module "Plugin-Interfaces"), • functions for user-profile data storage (module "CredentialStore"), • logging functions (module "logging"), and • auxiliary functions, such as data conversion (module "Utilities").
MigSafe	The subsystem MigSafe includes • a definition of the interfaces of the CS to the subsystem MigSafe of the TOE (module „MS-Interfaces“), • accesses the long-term-storage via the the module Plugin-Interfaces of the subsystem Common, • the validation of data objects with a XML-Schema (module „Validiation“), • the filtering of XML-documents (module „Filter“).
OverSign	The subsystem “OverSign” provides primarily functions for the preservation and renewal of the evidentiary value of electronic signatures and the integrity of the archived data objects.

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 Exact Description of the evaluated TOE configuration

The TOE as identified in section 2 has been evaluated. The TOE has been tested in the following configurations:

- TOE as delivered to customer / integrator

7.2 Developer's Test according to ATE_FUN

The developer considered the TOE environment as defined in the Security Target. The developer tests cover the following subsystems:

- Subsystem S1: MigSafe,
- Subsystem S2: OverSign and

- Subsystem S3: Common

and the following TSF interfaces:

- External Programming User Interface (EPUI) for client software.

Moreover, mechanisms of the security architecture of the TOE are also covered by tests. Each test is implemented as an automatic test based on the JUnit test framework and is executed on both operating systems RHEL 5.6 and 6.0. In addition a small subset of tests requires manual interaction.

The test documentation consists of a test coverage and depth of testing analysis, test plans for each of the test aspects (SF1, SF2, SF3, SF4, Integrity) and test result logs. The test plans show the goal, execution, test steps and expected results of the tests. The test result logs show that the tests identified in the test coverage and depth of testing analysis (if not redundant to other tests) have been executed as expected by the developer or are covered by manual tests.

7.3 Evaluator Tests

7.3.1 Exact Description of the Test configuration

The following test resources were used for the evaluator's testing within the environment of TÜViT:

- HW:
  - Intel Core2 Quad Core CPU Q8200 @ 2.33 GHz
  - 4 GB main memory
  - 750 GB hard disk space
  - Internet connectivity for access to time stamping provider and certificate status information
- SW:
  - RHEL 5.6/6.0 64bit
  - JDK 1.6.0_24 x64
  - Eclipse Platform 3.5.2
  - Eclipse project zip file containing the developer tests
  - JUnit version 4.8.2 (integrated in Eclipse project)
  - Configuration file for crypto component (siqVirtualTerminal.cfg)
  - OpenLimit Middleware Version 3 Server 1.2.0-2012022801 (x86_64)

7.3.2 Independent Testing according to ATE_IND

The functional testing was performed using the test environment of the CLEF. All configurations (RHEL 5.6/6.0 64bit) of the TOE being intended to be covered by the current evaluation were tested. The overall test result is that no relevant deviations were found between the expected and the actual test results.

Functional testing approach:

The developer provided the TOE which the evaluator installed on a test machine. The configuration of hardware and software on the test machine is consistent with the Security Target.

TOE test configurations:

The TOE as delivered to the customer has been tested.

Subset size chosen:

All interfaces of the TOE Security Functions (i.e. the interface to the Client Software) as well as all Security Functions are covered by independent functional tests.

Developer tests performed:

All automated developer tests have been repeated. The non-automated tests cover only a small subset of the overall functionality and have therefore not been repeated.

Verdict for the activity:

The overall test result is that no relevant deviations were found between the expected and the actual test results. No attack scenario was actually successful in the TOE's operational environment, see below.

7.3.3 Penetration Testing according to AVA_VAN

The penetration testing was performed using the test environment of the CLEF. All configurations of the TOE being intended to be covered by the current evaluation were tested. The overall test result is that no relevant deviations were found between the expected and the actual test results; moreover, no attack scenario was actually successful.

Penetration testing approach:

The developer provided the TOE which the evaluator installed on a test machine. The configuration of hardware and software on the test machine is consistent with the Security Target.

TOE test configurations:

The TOE as delivered to the customer has been tested.

Attack scenarios having been tested:

The four different attack scenarios having been tested are covering e.g. the authentication process and unexpected input values.

SFRs penetration tested:

All SFRs have been penetration tested with an emphasis on the authentication functionality of the TOE.

Verdict for the sub-activity:

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

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

The version information and hash values of the TOE as depicted in Table 2: Deliverables of the TOE executed with Java SDK 1.6.0_24 in its 64 bit version on the operating systems RHEL 5.6 and RHEL 6.0 64bit (see chapter 7.3.1 for further details).

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [8] 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.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 1.0, 31 October 2008, BSI-CC-PP-0049-2008 [7]
- for the Functionality: PP conformant
  Common Criteria Part 2 conformant
- 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 4, Para. 3, Clause 2). This holds for:

- SHA-256 according NIST FIPS Pub. 180-3 [12]
- RSA signature algorithm according PKCS#1 [11] with key length from 2048 to 4096 Bit

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 for 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.

As the TOE is a set of jar files that have to be integrated in a software component by the TOE integrator, it is of utterly importance that the integrator follows the guidelines as given in the integrator manual part of the file MigSafeOverSign-V1.0_Documentation.tgz referenced in Table 2: Deliverables of the TOE

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

ADO Archive Data Object

AOID Archive Object IDentifier

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

CLEF Commercial Licensed Evaluation Facility

CS Client Software

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

JDK Java Development Kit

PP Protection Profile

RHEL Red Hat Enterprise Linux

SAR Security Assurance Requirement

SDO Submission Data Object

SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
ST	Storage Unit
TOE	Target of Evaluation
TSF	TOE Security Functionality
TÜViT	TÜV Informationstechnik GmbH

12.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

Protection Profile - An implementation-independent statement of security needs for a TOE type.

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 - A set of software, firmware and/or hardware possibly accompanied by guidance.

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 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[11]

[5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0685-2012, Version 1.8, 10.07.2012, Security Target for SecDocs Security Komponenten Version 1.0, OpenLimit SignCubes GmbH

[7] Common Criteria Protection Profile for an ArchiSafe Compliant Middleware for Enabling the Long-Term Preservation of Electronic Documents Version 1.0, 31 October 2008, BSI-CC-PP-0049-2008

[8] Evaluation Technical Report, Version 5, 02.08.2012, TÜV Informationstechnik GmbH, (confidential document)

[9] Configuration list for the TOE, 10.07.2012, EVG-CM-List.xls (confidential document)

[10] Guidance documentation for the TOE as part of MigSafeOverSign-V1.0_Documentation.tgz: SecDocs Security Komponenten Version 1.0 – Handbuch für Integratoren, Version 2.3, 24.07.2012 and SecDocs Security Komponenten Version 1.0 – Handbuch für Administratoren, Version 2.0, 20.07.2012

[11] PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, 14. June 2002

[12] Federal Information Processing Standards Publication, FIPS Pub. 180-3, Secure Hash Standard (SHS), U.S. Department of Commerce / National Institute of Standards and Technology, October 2008

[11] specifically

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

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

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

Assurance Class	Assurance Components
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 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.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
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”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“Objectives

EAL1 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.

EAL1 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.

EAL1 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 EAL1 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 (EAL2) - structurally tested (chapter 8.4)

“Objectives

EAL2 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.

EAL2 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 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 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 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL4 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. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 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 (EAL5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL5 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 EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 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 (EAL6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL6 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.

EAL6 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 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL7 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 EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

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.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.