# Certification Report

**Bundesamt für Sicherheit in der Informationstechnik**

## BSI-DSZ-CC-0314-2005

## for

## S-TRUST Sign-it base components 2.0, Version 2.0.0.1

## from

## OPENLiMiT SignCubes AG

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 228 9582-0, Fax +49 228 9582-455, Infoline +49 228 9582-111

**Deutsches IT-Sicherheitszertifikat**

erteilt vom
Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

**BSI-DSZ-CC-0314-2005**

Signature application component

## S-TRUST Sign-it base components 2.0, Version 2.0.0.1

from

## OPENLiMiT SignCubes AG

Common Criteria Arrangement
for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Part 1 Version 0.6*, *Part 2 Version 1.0* extended by advice of the Certification Body for components beyond EAL4 for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)* and including final interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

**Evaluation Results:**

| | |
|---|---|
| Functionality: | **product specific Security Target**<br>**Common Criteria Part 2 extended** |
| Assurance Package: | **Common Criteria Part 3 conformant**<br>**EAL4 augmented by**<br>**AVA_MSU.3 – Analysis and testing for insecure states**<br>**AVA_VLA.4 – Highly resistant** |

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.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 21. Oktober 2005

The President of the Federal Office
for Information Security

Dr. Helmbrecht L.S.

IT Security Certified

SOGIS - MRA

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2)

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.

# 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 setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

# 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)
- Common Criteria for IT Security Evaluation (CC), Version 2.1[5]
- Common Methodology for IT Security Evaluation (CEM)
  - Part 1, Version 0.6
  - Part 2, Version 1.0
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

The use of Common Criteria Version 2.1, Common Methodology, part 2, Version 1.0 and final interpretations as part of AIS 32 results in compliance of the certification results with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2 as endorsed by the Common Criteria recognition arrangement committees.

[2] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

[3] Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 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 22nd September 2000 in the Bundesanzeiger p. 19445

# 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 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

## 2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, the Czech Republic in September 2004, the Republic of Singapore in March 2005, India in April 2005.

This evaluation contains the components AVA_MSU.3 and AVA_VLA.4 that are not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4-components of these assurance families are relevant.

# 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 S-TRUST Sign-it base components 2.0, Version 2.0.0.1 has undergone the certification procedure at BSI.

The evaluation of the product S-TRUST Sign-it base components 2.0, Version 2.0.0.1 was conducted by T-Systems GEI GmbH. The T-Systems GEI GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor is:

OPENLiMiT SignCubes AG
Zuger Str. 76 b
CH 6341 Baar, Switzerland

The developer of the TOE is:

OPENLiMiT SignCubes GmbH
Saarbrücker Str. 38 a
10405 Berlin, Germany

The distributor of the TOE is:

Deutscher Sparkassen Verlag GmbH
Am Wallgraben 115
70565 Stuttgart, Germany

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 21. Oktober 2005.

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, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

[6] Information Technology Security Evaluation Facility

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

# 4 Publication

The following Certification Results contain pages B-1 to B-31.

The product S-TRUST Sign-it base components 2.0, Version 2.0.0.1 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the sponsor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] OPENLiMiT SignCubes AG
Zuger Str. 76 b
CH 6341 Baar, Switzerland

This page is intentionally left blank.

# B Certification Results

The following results represent a summary of

- the security target of the vendor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

# Contents of the certification results

# 1 Executive Summary

The Target of Evaluation (TOE) and subject of the Security Target (ST) is the software application S-TRUST Sign-it base components 2.0, Version 2.0.0.1[8].

S-TRUST Sign-it base components 2.0 is an electronic signature application compliant to the German electronic signature law[9] and ordinance on electronic signatures[10]. The application itself is a set of executables and programming libraries. This means that S-TRUST Sign-it base components 2.0 may be used as a single application but also may be integrated into third party products.

The S-TRUST Sign-it base components 2.0 are provided by OPENLiMiT and are a branding version of the OPENLiMiT SignCubes base components 2.0.

The S-TRUST Sign-it base components 2.0 have been developed for the use on the operating systems from Microsoft since Microsoft Windows 98 SE. In the IT-security environment a smart card terminal with secure pin entry mode as well as a smart card are required to run the required cryptographic operations in the process of electronic signature creation.

The product does provide additional cryptographic functionality like data encryption based on symmetric encryption algorithms. These product capabilities are not part of the Common Criteria evaluation of this product.

The TOE itself is limited to the creation of hash values, using the SHA-1, SHA-256, SHA-384, SHA-512 and RIPEMD 160 algorithms and is therefore able to check and ensure the integrity as well as the trustworthiness of signed data based on the components responsible for CRL-processing, OCSP-processing, timestamp processing and PDF processing.

The TOE provides a legal binding displaying unit (S-TRUST Sign-it Viewer) for the Text, TIFF and PDF format. The displaying unit of the TOE allows the examination of the files content in order to ensure that the user is assured about the content to be signed or the content of the signed file.

The IT product S-TRUST Sign-it base components 2.0, Version 2.0.0.1 was evaluated by T-Systems GEI GmbH. The evaluation was completed on 20.10.2005. The T-Systems GEI GmbH is an evaluation facility (ITSEF)[11] recognised by BSI.

[8] Also named S-TRUST Sign-it base components 2.0 in this report

[9] see [10]

[10] see [11]

[11] Information Technology Security Evaluation Facility

The sponsor is

OPENLiMiT SignCubes AG
Zuger Str. 76 b
CH 6341 Baar, Switzerland

The developer is

OPENLiMiT SignCubes GmbH
Saarbrücker Str. 38 a
10405 Berlin, Germany

The TOE is exclusively distributed by

Deutscher Sparkassen Verlag GmbH
Am Wallgraben 115
70565 Stuttgart

## 1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see part C of this report,or [1], part 3 for details).

The TOE meets the assurance requirements of assurance level EAL4+ (Evaluation Assurance Level 4 augmented). The augmentation consists of the assurance requirements AVA_MSU.3 and AVA_VLA.4[12]

## 1.2 Functionality

The TOE provides the following functionality:

*Hash value computation and initiation of the electronic signature creation process using certificates, smart-card terminals and secure signature creation devices.*

The TOE computes hash values of any file or data buffer using the SHA algorithm family (SHA-1, SHA-256, SHA-384, SHA-512 and RIPEMD-160). After the hash value computation, the TOE uses the PC/SC or CT API or a card terminal vendor specific module to initiate the electronic signature creation by a secure signature creation system, which consists of a smart-card terminal and a smart card. The electronic signature is computed using the RSA algorithm, which is implemented as a part of the SSCD’s functionality. The TOE adds the signer certificate to the resulting document. Through the electronic signature, the data authentication is ensured. Through the addition of the signer certificate, the possibility of data verification is offered.

[12] In accordance with the German Signature Law (SigG) §17 paragraph 2 and the ordinance on electronic signatures (SigV) §15 paragraph 2 and paragraph 4.

Before the computation of the hash value starts, the TOE displays an unambiguous message, that an electronic signature should be created. It is unambiguous, to which data the electronic signature refers. Through the combination of a secure pin entry device and a smart card it is guaranteed that authorized persons only perform the electronic signature creation and identification data is not abandoned.

The user has the possibility to include an OCSP response for the user certificate that is used for the creation of the electronic signature into the resulting PKCS#7 encoded file or data buffer.

The TOE offers the possibility to add a timestamp into the PKCS#7 encoded file or data buffer that is the output of this TSF.

*Verification of hash values and electronic signatures using certificate revocation lists, OCSP responses (optional) and timestamps (optional)*

The TOE is able to verify electronic signatures that are based on a SHA-1, SHA-256, SHA-384, SHA-512 or RIPEMD 160 hash value. In this process it is unambiguous, to which data the electronic signature refers. For the purpose of electronic signature verification, the hash value of the signed data is computed, using the SHA algorithm family or the RIPEMD 160 algorithm and the original hash value extracted from the signature using the RSA algorithm and the public key of the given signer certificate. In addition to this operation, the certificate chain is checked, using the chain model or RFC 3280.

The TOE displays an unambiguous message, whether the hash values were identical or not. Because of this, it is unambiguous, whether the original data has changed or not. The correctness of the electronic signature is reliably checked and displayed. Through the use of the S-TRUST Sign-it Viewer component it is ensured, that the content of the signed data is unambiguously displayed.

The TOE offers the possibility to identify the user that has generated the electronic signature based on the certificate that has been used. The user, who verifies the validity of the electronic signature by using the TOE, has the possibility to view the certificate that has been used for the generation of the electronic signature in an unambiguous way.

During the verification process, the issuer of the signers certificate is determined and a corresponding certificate revocation list is loaded. This revocation list is checked, if a revocation entry for the signers certificate exists. If this is the case, this information is taken. If the certificate was already revoked during the signature creation, this information is displayed to the user.

In addition to the checking of the revocation list the user has the possibility to use an OCSP response to verify the validity of a certificate under examination. The OCSP response may be encoded in the PKCS#7 data under examination or is requested from an OCSP responder using software modules that are not part of the evaluation.

Also the user has the possibility to use a given time stamp that is encoded in the PKCS#7 data at the point of time where the signature has been created. The time stamp may be part of the PKCS#7 encoded data under examination or is presented to the TOE as a separate file. The timestamp can be used by the TOE to provide validity information for the signature under examination at the point of time that is specified by the timestamp.

The basic validity checking is always done using the time that is encoded in the PKCS#7 data block. This time is normally the system time when the signature has been created. If no time of signature creation is available, the current system time is used as the point of time of signature creation.

*Program module manipulation detection*

The TOE is delivered with electronically signed libraries, files and executables. In order to implement the required functionality of manipulation detection, a separate program module is implemented as dynamic linked library (dll). All subsystems of the product know the SHA-512 hash value of this check module. The check module knows the public key, whose counterpart (the private key) was used to sign the program libraries, files and executables.

If the S-TRUST Sign-it base components 2.0 are started, the S-TRUST Sign-it Security Environment Manager checks its environment using the check module. In step 1, the Security Environment Managers validates the hash value of the check module. In step 2, the check module verifies the application, which loads the check module, by verifying the electronic signature of the loading application mathematically.

If a dynamic module should be loaded by the application, the check module is always used to verify the integrity of the module to be loaded. Therefore the check module computes the hash value of the module to be loaded and verifies the electronic signature of the module to be loaded mathematically. If the verification fails, the check module sends a signal to all program modules, which are now deactivated. Using this mechanism, no security related operation could be performed using the product.

All modules of the application know the hash value of the check module. If the hash value of the check module cannot be validated, the modules can no longer be used.

*Unambiguous presentation of the data to be signed*

The TOE ensures that the content of displayed document is unambiguous. In addition to this, the user is informed, if the data contains hidden or active content or content that cannot be displayed.

The file that should be signed must be a Text, Tiff or PDF formatted file. An appropriate parser explores the type of the data. If the parser is unable to determine the type of the data an appropriate error message is displayed that contains a hint that the data could not be displayed. After this first operation the data is checked for hidden and active content. If the file contains unknown tags, elements or control characters the user is informed that the file may contain unintended content. If the parser detects active or hidden content an appropriate message is displayed to the user that informs him about this state. If the user wants to display the file and the file contains hidden content or content, that cannot be displayed, a warning message is generated and displayed to the user.

*Protection against hash value manipulation*

Before the process of electronic signature creation starts, the hash value using the SHA algorithm family is used. Alternatively the RIPEMD 160 algorithm may be used. After the electronic signature creation process, the TOE verifies the electronic signature using the public key of the given signer certificate. If the original hash value and the hash value encoded in the electronic signature are not identical, the hash value was corrupted during the transmission to the secure signature creation device. After this operation, an unambiguous message is displayed, if the correct data has been signed.

*Assurance of the TOE's integrity*

The integrity of the TOE can be ensured by the user using the check utility, which could be accessed online. This check utility is a Java Applet, which ensures the integrity of the application by checking and comparing the SHA-1 hash values of the program modules. Therefore the hash values are known to the Applet.

The Java Applet is a signed Java Archive (with the extension JAR), the integrity of the Applet itself is ensured by the mechanisms of the Java Virtual Machine (JVM). Therefore the user is required to install a Java Virtual Machine. The JVM must be at least compatible with the Java Runtime Environment 1.4 from Sun.

The user must use a dialog to point to the current installation path of the product or uses the installation directory detected by the S-TRUST Sign-it Integrity Tool from the registry. The integrity check does not verify any registry entries.

The integrity check utility is aware of the root certificates contained in the certificate trust lists, which were initially installed.

If the computed hash values and the expected hash values of the program modules are not identical, an error message is generated and displayed to user in an unambiguous way. If no differences in the configuration were detected, the check utility displays an unambiguous dialog with an appropriate summary.

*Processing of OCSP information for certificate validation*

The TOE offers the possibility to process OCSP information in order to verify the validity of a certificate. This certificate is called 'certificate under examination'. In order to use the validity information that is provided for the certificate under examination through the OCSP response, the TOE is required to verify the electronic signature of that response.

The OCSP response might be part of a PKCS#7 encoded signature block, a plain file or is received through an appropriate OCSP handler. In the process of OCSP response import the TOE verifies the validity of the OCSP response through the mathematical verification of the electronic signature that belongs to the OCSP response. Mathematical verification means that the OCSP response must contain a signature from the certificate that is included in the OCSP response as the OCSP response signing certificate and the signature must be valid. During the import the TOE does not check the complete certificate chain. If the TOE is not able to verify the signature, the OCSP response is not imported and an appropriate message is displayed to the user. After the import process the TOE is also able to store the OCSP response in a PKCS#7 encoded file or in a separate file.

When the TOE uses the OCSP information for certificate validation a complete verification of the OCSP signature based on certificate revocation lists is required. The signature might be based on a SHA-1, SHA-256, SHA-384, SHA-512 or RIPEMD 160 hash value. For the purpose of electronic signature verification, the hash value of the signed data is computed, using the SHA algorithm family or the RIPEMD 160 algorithm and the original hash value extracted from the signature using the RSA algorithm and the public key of the OCSP response signing certificate. In addition to this operation, the certificate chain for that OCSP signing certificate is checked, using the chain model or RFC 3280. All certificates in the chain are checked for revocation information that is provided by appropriate CRL’s.

After the validation of the electronic signature the TOE displays an unambiguous dialog to the user that informs him about the validity of the OCSP response and the validity information for the certificate under examination extracted from that OCSP response. In addition to that the TOE provides a second dialog that provides detailed information about the content of the OCSP response, including the certificate that has signed the response.

The validity information that is based on the OCSP response for the certificate under examination might be used in the process of signature verification to determine the validity of a certificate under examination.

*Application of Timestamps*

The TOE offers the possibility to apply timestamps to files. Therefore an external timestamp handler is used in order to receive the timestamp, the correctness of the timestamp itself is ensured by the TOE.

In the process of timestamp import the TOE verifies the electronic signature of the timestamp using the public key of the certificate that has signed the timestamp. The certificate must be known to the TOE in order to verify the signature, otherwise the TOE would not import the timestamp.

The signature might be based on a SHA-1, SHA-256, SHA-384, SHA-512 or RIPEMD 160 hash value. For the purpose of the mathematical validation, the hash value of the signed data is computed, using the SHA algorithm family or the RIPEMD 160 algorithm and compared with the original hash value extracted from the signature using the RSA algorithm and the public key of the timestamp signing certificate.

After importing the timestamp, the timestamp is applied to the file that has been chosen by the user. Application means the encoding of the timestamp into an existing PKCS#7 encoded file or the storage of the timestamp in a separate file.

*Validation of Timestamps*

In the process of timestamp validation the TOE verifies the electronic signature of the timestamp with the public key that has signed the timestamp. The certificate must be known to the TOE in order to verify the signature, otherwise the TOE is unable to validate the timestamp. The signature might be based on a SHA-1, SHA-256, SHA-384, SHA-512 or RIPEMD 160 hash value. For the purpose of the mathematical validation, the hash value of the signed data is computed, using the SHA algorithm family or the RIPEMD 160 algorithm and compared with the original hash value extracted from the signature using the RSA algorithm and the public key of the timestamp signing certificate. In addition to this operation, the certificate chain for that timestamp signing certificate is checked, using the chain model or RFC 3280. All certificates in the certificate chain are checked for revocation information provided by appropriate CRL's.

The result of the timestamp validation is displayed to user through a dialog that is provided by the TOE. This dialog provides the information that is encoded in the timestamp and does also provide the capability to display the certificate that signed the timestamp.

*Management of Security Functions depending on licenses*

The TOE implements a licensing mechanism that allows the management of security functionality in the product.

Each time the TOE is started it validates its license. If no license file is found, the TOE displays a dialog and requests the user to enter a license number that he received together with the TOE's setup routine. The license number encodes information about the product capabilities under the aspect of PDF displaying and the ability to initiate the computation of an electronic signature. The electronic signature initiation and PDF operating modes that depend on the license are defined as following:

- Mode 1: No signature creation capabilities of the TOE, if the user does not have a license code. The displaying of PDF documents is not allowed.
- Mode 2: No PDF displaying capabilities of the S-TRUST Sign-it Viewer. No possibilities to create any kind of signature on PDF documents. The S-TRUST Sign-it Viewer can be utilized to display Text and TIFF documents and to create PKCS#7 signatures on these document types.
- Mode 3: PDF displaying but no capabilities to create signatures on PDF documents using the S-TRUST Sign-it Viewer. PKCS#7 and embedded PDF signatures on PDF documents can be verified. The S-TRUST Sign-it Viewer can be utilized to display Text and TIFF documents and to create PKCS#7 signatures on these document types.

- Mode 4: PDF displaying and the capability to create attached and detached PKCS#7 signatures as well as the verification of these signatures using the S-TRUST Sign-it Viewer45. The S-TRUST Sign-it Viewer can be utilized to display Text and TIFF documents and to create PKCS#7 signatures on these document types. The capability to create PDF signatures is no enabled
- Mode 5: PDF displaying is enabled, the creation of PKCS#7 encoded and PDF signatures for PDF documents is enabled as well as the verification of these signature types. The S-TRUST Sign-it Viewer can be utilized to display Text and TIFF documents and to create PKCS#7 signatures on these document types.

If the user has not entered a license code, the TOE extracts a license file that enables Mode 1. In this case the generation of an electronic signature is not required. This license file is signed and uses no hardware binding, because for Mode 1 this binding is not required.

After the hash value computation over the resulting license file, the TOE uses the PC/SC or CT API or a card terminal vendor specific module to initiate the electronic signature creation by a secure signature creation system, which consists of a smart-card terminal and a smart card. The electronic signature is computed using the RSA algorithm, which is implemented as a part of the SSCD’s functionality. The TOE adds the signer certificate to the resulting document. Through the electronic signature, the data authentication is ensured. Through the addition of the signer certificate, the possibility of data verification is offered and the evidence of the user who has signed the license file is added.

When the TOE is started the next time it verifies the licensing information together with the binding on the hardware. Therefore the TOE verifies the electronic signature on the license file with the public key that has been used for the generation of the electronic signature. In conjunction with this operation the TOE sets up the certificate chain up to a trusted certificate that must be located in a certificate trust list file that contains all root and CA certificates that are trusted as certificates for issuing user certificates to be accepted by the TOE.

After this operation the found licensing information is used to enable the capabilities that have been defined to be manageable in the TOE.

The TOE offers an appropriate dialog that informs the user about:

- The licensed functionality
- The serial number
- The certificate that has been used to enable the license on the users computer

The same dialog provides the functionality to update the license by repeating the licensing procedure of the TOE. In the case that the user has utilized license mode 1 and the user repeats the licensing process or generates the license for the first time, the TOE allows the creation of an electronic for that purpose.

The certificate that has been used for the creation of the electronic signature provides the evidence of the user that has enabled the product features.

The S-TRUST Sign-it Job Interface is allowed to utilize the TSF of the TOE, even if these capabilities are not part of the users license. Therefore the TOE contains a certificate in its resources that is used in this case to verify the electronic signature of that external module. This external module is not signed with the same key as the TOE.

The S-TRUST Sign-it base components 2.0 have been developed for the use on the operating systems from Microsoft since Microsoft Windows 98 SE. Cryptographic operations for the creation of digital signatures are conducted securely by means of the IT-environment (smart card and smart card reader with PIN-Pad). Therefore, the IT-environment must comprise a smard card reader that provides a secure entry mode for the PIN and a smart card.

The product S-TRUST Sign-it base components 2.0 is compliant to the signature law (SigG) §17 paragraph 2 and to the ordinance on electronic signatures (SigV) §15 paragraph 2 and paragraph 4.

## 1.3 Strength of Function

The TOE's strength of functions is claimed high (SOF-high).

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2) (see Chapter 9 of this report).

## 1.4 Summary of Threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The analysis of security threats to the TOE and to objects, which should be protected by the TOE were supplemented using the document "Maßnahmenkatalog für technische Komponenten nach dem Signaturgesetz" [12] though this catalogue to the outdated signature law (from 22.07.1997). The usage of this catalogue is tolerable, because the arrangements can be implied to the current signature law.

In addition to that the CEN Workshop Agreement CWA 14170 "Security Requirements for Signature Creation Applications" has been used for the analysis of security threats.

All security threats assume an adversary with high attack potential. For the protection against the threats identified in this section the kind of exploited vulnerability is irrelevant because the identified threats should be prevented in general.

Objects that must be protected by the TOE are: the document that the user wants to sign ("user file"), a signed file and the TOE with its own data and files.

*User File*
A user file is a file that user decided to sign with the TOE and that is currently processed by the TOE. Currently processed means that the TOE holds a kind of reference to that file expressed by the directory and the name of the file.

*Signed File*

A Signed File is a file with an electronic signature.

*TOE's data and files*

This term means all binary and configuration files of the TOE. The term data refers to files that are required to operate the TOE correctly, e.g. certificates.

The ST lists the following threats to security in chapter 3.2:

**T.DAT**

*Manipulation of a user file*

The adversary manipulates a user file using any instrument and the manipulation is not detected.

This security threat is very general, because several scenarios are covered through this. The term user file has been defined in the section above. The adversary may manipulate the file using an appropriate file editor, a network tool or any other applicable mechanism. A manipulation covers random manipulations as well as systematic changes to the file.

**T.SIG_DAT**
*Manipulation of a signed file*

The adversary manipulates a signed file using any instrument and the manipulation is not detected.

This security threat is very general, because several scenarios are covered through this. The definition of the term signed file has been given in the section above. The adversary may manipulate the file using an appropriate file editor, a network tool or any other applicable mechanism. A manipulation covers random manipulations as well as systematic changes to the file.

**T.TOE**
*Manipulation of the TOE and of its files*

The adversary manipulates or replaces parts (modules) or data of the TOE on the computer and the manipulation is not detected.

The manipulation of TOE files or modules is a direct attack against the product. The adversary manipulates or changes parts of the TOE with the scope, to change some of the security functionality or even to deactivate this functionality of the TOE.

**T.PRE_SIG**

*Manipulation of a file before the users decision to sign the file*

The adversary changes the file using any mechanisms, before the user decides to sign the file and the manipulation are not detected.

The file is a file that the user wants to sign. The security threat implies an adversary who is able to change files in the time between the selection of the file16 and the beginning of the signing process.

### T.POST_SIG

*Creation of a falsified electronic signature*

The adversary manipulates the computed hash value of the document before the hash value is transmitted to the secure signature creation device and the manipulation is not detected.

The adversary is able to manipulate the hash value of the data to be signed in the time slice between the start of the signature process triggered by the user and the transmission to the smart card. It may be possible, to change the hash value of the data during transmission to the secure signature creation device.

### T.LIC

*Downgrading of TOE's manageable capabilities*

The adversary utilizes a license code or license file that disables parts of the TOE's manageable capabilities and this downgrading is not detected.

The adversary owns a license code or a license file for the TOE that enables a smaller set of capabilities of the TOE that are managed through the license code and enters this license code. The TOE would not provide the full set of functionality the user has licensed.

### Organizational Security Policies

There are no organizational security policies defined for the TOE.

## 1.5 Special configuration requirements

The TOE is a software application. The different parts of the application (executable programs and dynamic link libraries) are identified in the configuration list [8]. The configuration of the TOE and the technical environment can be deduced from the ST [6]. Further information about the configuration is also provided in this report in chapter 1.6, chapter 4.2 and chapter 8.

Detailed information about the configuration of the TOE is also provided in the user guidance [9]

## 1.6 Assumptions about the operating environment

The TOE will be used only on dedicated hardware platforms based on different operationg systems of the Microsoft Windows family. Furthermore, several assumptions of the operating environment and the personnel using the TOE are mentioned in the ST [6].

For a concise description of assumptions see chapter 4.1, chapter 4.2 and chapter 8 of this report.

## 1.7 Disclaimers

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

As stated above, the Target of Evaluation is called S-TRUST Sign-it base components 2.0, Version 2.0.0.1.

The following table summarises the deliverables of the TOE and thus the evaluated configuration.

| No. | Type | Description | Version | Date | Delivery |
|---|---|---|---|---|---|
| 1. | Software | S-TRUST Sign-it base components 2.0 | 2.0.0.1 | 19.10.2005 | File |
| 2. | Documentation | S-TRUST Sign-it 2.0 Benutzerdokumentation | 2.0.0.1 | 19.10.2005 | chm-File |
| 3. | Header File | siqSDK.h | | 19.10.2005 | File |
| 4. | Library File | siqSDK.lib | | 26.09.2005 | File |

**Table 1: Deliverables of the TOE**

To identify the Header and Library Files the SHA-1 values of these files are listed in the next table.

| No. | File | SHA-1-value |
|---|---|---|
| 1. | siqSDK.h | 1ed950b3c89439519d2f001104b831e72cd93832 |
| 2. | siqSDK.lib | 9861b0eec3daa97c8522b449a4fd6008d190cfdc |

**Table 2: Hash Values of TOE deliverables**

The TOE deliverables No.1 and No.2 are provided for a customer, who purchases the TOE as a standalone application. The TOE deliverables No.3 and No.4 are delivered additionally and have to be purchased separately. They are intended for developers who want to integrate the API provided by the TOE into their own application.

# 3 Security Policy

The TOE is compliant to  the German signature law and ordinance on electronic signature and thus enforces the following security policies:

- The TOE clearly indicates the production of a qualified electronic signature and enables the data to which the signature refers to be identified.
- The TOE ensures that the identification data are not disclosed and are stored only on the relevant secure signature creation device. The application enforces the rule that a signature is provided only at the initiation of the authorized signing person.
- The TOE shows, to which data the signature refers, whether the signed data are unchanged and to which signature-code owner the signature is to be assigned.
- The TOE presents the contents of the qualified certificate on which the signature is based, the appropriate qualified attribute certificates and the results of the subsequent check of certificates.
- If data to be signed or data already signed is displayed by the TOE certain rules for the treatment of not readable signs are enforced.
- For the verification of a qualified electronic signature the TOE reliably verifies the correctness of a signature and displays this fact appropriately.
- Using the TOE it can be clearly determined whether the verified qualified certificates were present in the relevant register of certificates at the given time and were not revoked.
- The TOE ensures, that security-relevant changes in the technical components are apparent to the user.

# 4 Assumptions and Clarification of Scope

## 4.1 Usage assumptions

According to the ST [6], chapter 3.1, the following assumption for the usage of the TOE is made:

- A.Personnel
  The user, the administrator and the maintenance staff are trustworthy and follow the user guide of the TOE. Especially the user verifies the integrity of the TOE as described in the user documentation.

## 4.2 Environmental assumptions

The ST mentions the following assumptions for the IT environment in chapter 3.1:

- A.Platform

  The user utilizes an Intel 586 compatible computer as hardware platform, which contains at least 64 MB of RAM and 60 MB of free disk space.

  On the computer is one of the following operating systems installed:

  - Windows 98 SE
  - Windows ME
  - Windows NT 4 SP 6
  - Windows 2000 SP 2
  - Windows 2003
  - Windows XP Home
  - Windows XP Professional
  - Windows XP Tablet PC Edition
  - Windows XP 64 Bit Edition

  In addition to these requirements, the Internet Explorer version 5.01 or higher is installed. Moreover, the Microsoft smart card base components are installed on the computer[13].

  In addition to that, a Java Virtual Machine (JVM) is installed on the computer, which complies at least with the Java Runtime Environment v1.4.

[13] The manual installation of the Microsoft SmartCard base components is required for Microsoft Windows 98 SE, Microsoft Windows ME and Microsoft Windows NT 4.0.

The user ensures, that all components of the operating system are correct. The user ensures that no malicious or harmful program is installed on the system.

The user utilizes a secure signature creation system, which consists of a smart-card terminal with secure pin entry capabilities together with a smart card. The user utilizes one of the following SigG approved smart cards:

- ZKA Banking signature card, v6.2b NP and 6.2f NP, Type 3 from Giesecke & Devrient[14]
- ZKA Banking signature card v6.31 NP, Type 3 from Giesecke & Devrient[15]
- ZKA signature card, version 5.02 from Gemplus-mids GmbH
- S-TRUST signature card release 3 (SPK 2.3 based)

In addition to the listed smart cards, the user utilizes any smart card that provides a PKCS #15 interface or a SigG-application for qualified electronic signatures.

The user utilizes one of the following smart-card terminals:

- Cherry G83-6700 LQ
- Cherry G83-6744 LU
- Kobil Systems B1 Pro USB
- Kobil Systems KAAN SecOVID Plus
- Kobil Standard Plus
- Kobil KAAN Advanced
- SCM Microsystems SPR x32
- Reiner SCT cyberJack e-com v2.0
- Reiner SCT cyberJack pinpad v2.0
- Reiner SCT cyberJack pinpad v3.0
- Omnikey Cardman 3821
- Omnikey Cardman 8630

The used components are approved components according to the German signature law[16]. The certificates can be obtained from the Bundesnetzagentur (www.bundesnetzagentur.de).

[14] The approval has not yet been published by the Bundesnetzagentur.

[15] The approval has not yet been published by the Bundesnetzagentur.

- A.Network

  The computer, where the TOE is installed, may have Internet access. In this case a firewall is used to ensure, that no system services or components are compromised through internet attacks. In addition to this, the user utilizes a virus scanner, which is able to detect virus programs as well as backdoor programs and root kits. At least the virus scanner is able to inform the user about attacks or detected malicious programs.

- A.Access

  The computer, on which the TOE is installed, is located in an environment, where the user has full control about inserted storage devices and shared network storage places. The TOE is protected in such way, that it is not possible to access parts of the TOE or the TOE as a whole through existing network connections.

## 4.3 Clarification of scope

The TOE cannot assure the correctness of the following functions:

- Private Key material. The secure signature creation device must assure the correctness and integrity of the private key material.
- Assurance of the operating system integrity. The TOE does not contain any capabilities for ensuring the integrity of the operating system and its environment. The user must assure, that sufficient actions are undertaken to avoid, that the operating system may be compromised.
- Strength and security of cryptographic operations. The TOE uses libraries for hash value creation and the RSA algorithm for signature validation. Therefore the TOE can only assure the compliance to given standardization documentation and test vectors but must not make any statement about the strength of the cryptographic operations.

The capability characteristics of the TOE are limited to the computation of hash values and the usage of secure signature creation devices for electronic signature creation and the usage of the RSA algorithm for signature verification. Manipulations on the IT-security environment cannot be recognized or even prevented by the TOE.

Applications that use the TOE via the evaluated API are **not** in the focus of this evaluation.

[16] with exception of the following ones: Kobil KANN Advanced, Omnikey Cardman 3821, Omnikey Cardman 8630.

**Restrictions and Exceptions**

Some combinations of smart card terminals, smart cards and operating systems that were listed in the assumption A.Platform do not work together. These combinations are:

- The smard card terminals Cherry G3-6744 LU, Kobil B1 Professional, Reiner SCT cyberJack pinpad v2, Reiner SCT cyberJack pinpad v3.0 and Omnikey Cardman 3821 are not supported by Microsoft Windows NT 4 SP 6.
- The smard card terminals Cherry G83-6700 LQ, Cherry G83-6744 LU, Kobil Systems B1 Pro USB, Kobil Systems KAAN SecOVID Plus, Kobil Standard Plus, Kobil KAAN Advanced, SCM Microsystems SPRx32/ChipDrive pinpad, Reiner SCT Cyber Jack e-com v2.0, Reiner SCT Cyber Jack pinpad v2.0 and Omnikey Cardman 8630 are not supported by Windows XP 64 Bit Edition.

**Those combinations of smard card readers and operating systems are not included in the evaluation and therefore not included in the certificate.**

Furthermore, the following restrictions hold true:

- The smart card terminal Kobil Systems B1 Pro USB does not support the ZKA-API.
- The smart card S-TRUST signature card release 3 (SPK 2.3 based) does not support the ZKA-API.

**Consequently, the evaluation results and the certificate for the smart card terminal Kobil Systems B1 Pro USB and smart card S-TRUST signature card release 3 (SPK 2.3 based) do not include the support of the ZKA-API.**

# 5 Architectural Information

The TOE is a signature application component compliant to the German electronic signature law and ordinance on electronic signatures. The application itself is a set of executables and programming libraries. This means that S-TRUST Sign-it base components 2.0 may be used as a single application but also may be integrated into third party products.

The TOE (see chapter 6.1 in the Security Target [6]) provides the following security functions:

SF.1 Hash value computation and initiation of the electronic signature creation process using certificates, smart-card terminals and secure signature creation devices.

SF.2 Verification of hash values and electronic signatures using certificate revocation lists, OCSP responses (optional) and timestamps (optional)

SF.3 Program module manipulation detection

SF.4 Unambiguous presentation of the data to be signed

SF.5 Protection against hash value manipulation

SF.6 Assurance of the TOE’s integrity

SF.7 Processing of OCSP information for certificate validation

SF.8 Application of Timestamps

SF.9 Validation of Timestamps

SF.10 Management of Security Functions depending on licenses

The TOE comprises three different parts:

- the S-TRUST Sign-it Security Environment Manager
- the S-TRUST Sign-it Viewer
- the S-TRUST Sign-it Integrity Tool

The first two parts represent the main components of the TOE whereas the S-Trust Sign-it Integrity Tool is is a separate application implemented as a Java Applet. The S-TRUST Sign-it Integrity Tool is used to allow the user to check the integrity of the installed product.

The figure below provides an overvierw of the main components and their interfaces as provided in the High-Level Design.

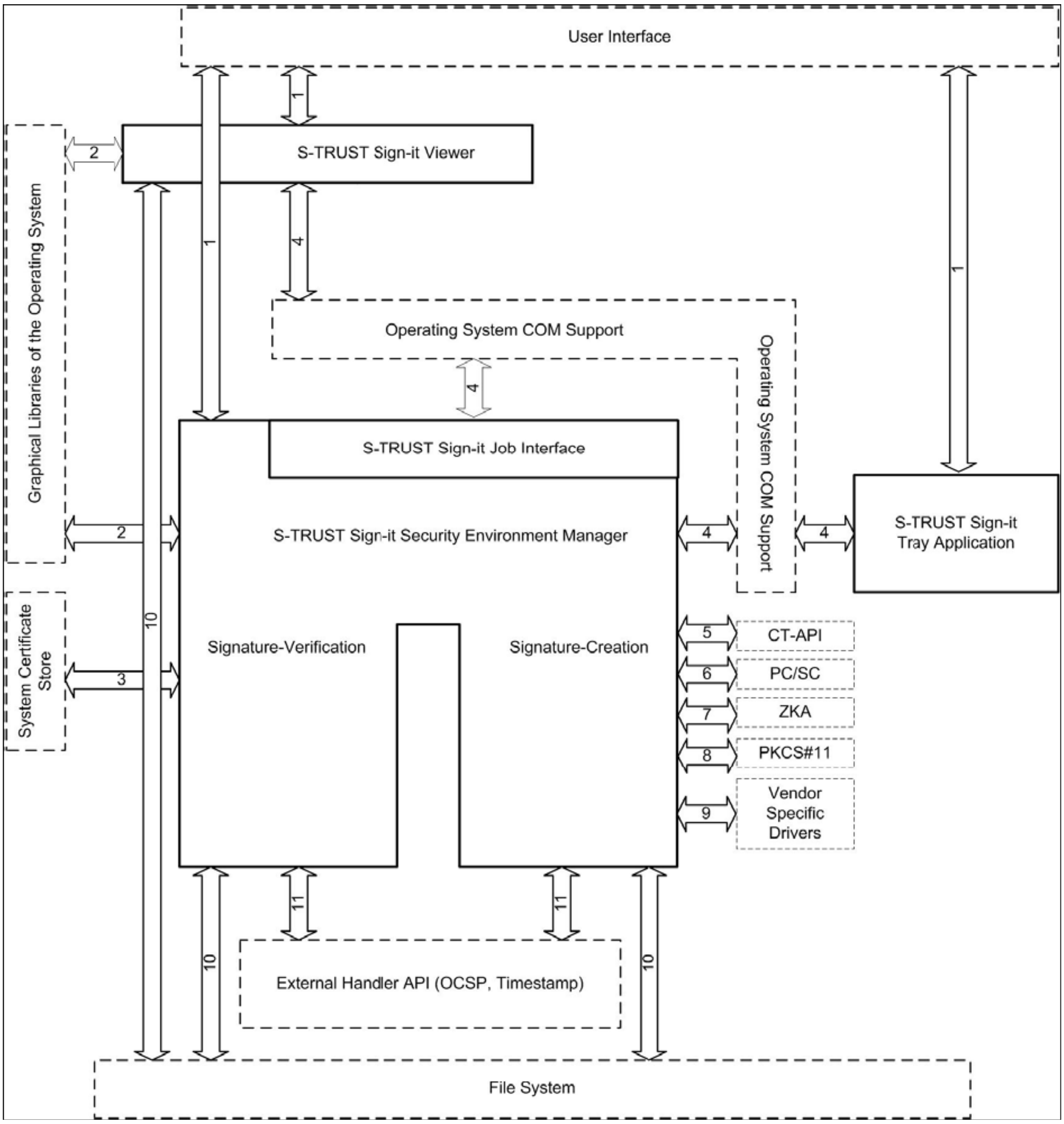
User Interface
1
S-TRUST Sign-it Viewer
2
Graphical Libraries of the Operating System
1
4
1
Operating System COM Support
4
S-TRUST Sign-it Job Interface
Operating System COM Support
S-TRUST Sign-it Security Environment Manager
2
4
4
S-TRUST Sign-it
Tray Application
10
Signature-Verification
Signature-Creation
5
CT-API
System Certificate Store
3
6
PC/SC
7
ZKA
8
PKCS#11
9
Vendor
Specific
Drivers
11
11
10
External Handler API (OCSP, Timestamp)
10
File System

**Figure 1: Decomposition of the main components of the TOE**

In Figure 1 the lined boxes represent the subsystems of the main components of the TOE whereas the arrows indicate interfaces between subsystems. Dashed boxes refer to external subsystems that are part of the IT environment of the TOE (see chapter 4.1 and chapter 4.2 in this report).

The S-TRUST Sign-it Viewer is a software component for displaying signed data or data to be signed according to the signature law §17 paragraph 2. The S-TRUST Sign-it Viewer is able to display TIFF documents following the Adobe TIFF specification, PDF documents that follow the PDF 1.6 document format as well as documents that contain ASCII characters. If the user decides to sign the document that is currently displayed with the S-TRUST Sign-it Viewer, he can start the process of electronic signature creation using the S-TRUST Sign-it

Viewer as an indirect interface to that functionality provided by the S-TRUST Sign-it Security Environment Manager.

The S-TRUST Sign-it Security Environment Manager provides the following functionality that may be accessed in parts or completely through the use of the S-TRUST Sign-it Job API:

- Computation of hash values using the SHA-1, SHA-256, SHA-384, SHA-512 and RIPEMD 160 algorithms.
- Creation of electronic signatures using a smart card and a secure pin entry device.
- Timestamp processing during the process of electronic signature creation.
- Support for attribute certificates in the process of electronic signature creation.
- Support for OCSP processing during the electronic signature creation.
- Electronic signature verification including OCSP and CRL processing as well as timestamp processing. The use of attribute certificates is supported.
- API's for applications/product parts that want to use the provided functionality.
- Ensuring the integrity and correctness of the SignCubes base components installed on the users computer.
- Providing graphical interfaces in the process of signature creation, verification and product configuration

# 6 Documentation

The product S-TRUST Sign-it base components 2.0 is provided with the following documentation:

The user guidance [9] contains important instruction about the operation of the TOE, installation, errors and usage.

In the ST [6] the user finds information about the security objectives of the TOE, threats and security functions to avert these threats. The Security Target is publicly available but not automatically shipped with the TOE.

# 7 IT Product Testing

The TOE S-TRUST Sign-it base components 2.0is uniquely identified by the contents of the configuration list [8]. All tests were conducted for the same version of the TOE.

## 7.1 Test configuration

The tests of the developer were conducted with the smard cards, smart card terminals and operating systems listed below in accordance with the ST [6]. All additional prerequisites mentioned in the assumptions on the operating environment (see chapter 1.6 and chapter 4.2 in this report) concerning the installation of modules of the operating systems (e.g. the correct version of the Internet explorer) or firewalls and virus scanners were fullfilled for the computers of the testbed.

**Smart cards**

- ZKA Banking signature card, v6.2b NP and 6.2f NP, Type 3 from Giesecke & Devrient
- ZKA Banking signature card v6.31 NP, Type 3 from Giesecke & Devrient
- ZKA signature card, version 5.02 from Gemplus-mids GmbH
- S-TRUST signature card release 3 (SPK 2.3 based)

**Smart card terminals**

- Cherry G83-6700 LQ
- Cherry G83-6744 LU
- Kobil Systems B1 Pro USB
- Kobil Systems KAAN SecOVID Plus
- Kobil Standard Plus
- Kobil KAAN Advanced
- SCM Microsystems SPR x32
- Reiner SCT cyberJack e-com v2.0
- Reiner SCT cyberJack pinpad v2.0
- Reiner SCT cyberJack pinpad v3.0
- Omnikey Cardman 3821
- Omnikey Cardman 8630

**Operating systems**

- Windows 98 SE
- Windows ME
- Windows NT 4 SP 6
- Windows 2000 SP 2
- Windows 2003
- Windows XP Home

- Windows XP Professional
- Windows XP Tablet PC Edition
- Windows XP 64 Bit Edition

## 7.2 Developer tests

The test description demonstrates that the developer performed his testing on an adequate level for the evaluation assurance level EAL4 augmented. For the Common Criteria evaluation very many tests were conducted. According to the verdict of the evaluator mentioned in the Evaluation Technical Report (ETR) [7], the test effort of the developer demonstrate that the security functionalities defined in the ST [6] have been implemented as required.

## 7.3 Evaluator tests

In context of the evaluation the ITSEF repeated some of the developer tests and performed independent tests in addition. The following testing approach was chosen: Independent tests were identified based on the developer tests already available. The developer tests have been compared with the ST, the FSP and the HLD in order to determine the fields of further investigation.

The tests showed, that the TOE behaves as expected. The depth of testing is adequate for the evaluation assurance level chosen (EAL4 augmented). The TOE has successfully passed independent testing.

The penetration tests performed by the evaluators confirmed that potential vulnerabilities found by the evaluators are not exploitable.

# 8 Evaluated Configuration

The TOE S-TRUST Sign-it base components 2.0 was evaluated in the configuration as described in the Evaluation Technical Report [7] and as summarized in chapter 2 of this report.

The TOE is delivered either via online download or via CD-ROM. The setup-program enclosed in the distribution enables the user to install the deliverables as required. After the installation the user is required to execute the S-Trust Sign-it Integrity Tool provided via download from the internet address https://www.s-trust.de/sign-it/sicherheit. Thus, the user ensures that the evaluated configuration is installed.

The TOE allows only one mode of operation though several different functionalities are bound to purchasing a corresponding license. Depending on the license, the user may use only parts of the functionality evaluated and certified. In any case, the evaluation and the certificate cover all functionalities that the purchase of the most comprehensive license provides.

# 9 Results of the Evaluation

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 those components identical with EAL4. For components beyond EAL4 the methodology was defined in co-ordination with the Certification Body [4, AIS 34]).

The verdicts for the CC, Part 3 assurance components (according to EAL4 augmented by AVA_VLA.4 and AVA_MSU.3 and the class ASE for the Security Target evaluation) are summarised in the following table.

| Assurance classes and components | | Verdict |
|---|---|---|
| Security Target evaluation | CC Class ASE | PASS |
| TOE description | ASE_DES.1 | PASS |
| Security environment | ASE_ENV.1 | PASS |
| ST introduction | ASE_INT.1 | PASS |
| Security objectives | ASE_OBJ.1 | PASS |
| PP claims | ASE_PPC.1 | PASS |
| IT security requirements | ASE_REQ.1 | PASS |
| Explicitly stated IT security requirements | ASE_SRE.1 | PASS |
| TOE summary specification | ASE_TSS.1 | PASS |
| Configuration management | CC Class ACM | PASS |
| Partial CM automation | ACM_AUT.1 | PASS |
| Generation support and acceptance procedures | ACM_CAP.4 | PASS |
| Development tools CM coverage | ACM_SCP.2 | PASS |
| Delivery and operation | CC Class ADO | PASS |
| Detection of modification | ADO_DEL.2 | PASS |
| Installation, generation, and start-up procedures | ADO_IGS.1 | PASS |
| Development | CC Class ADV | PASS |
| Semiformal functional specification | ADV_FSP.2 | PASS |
| Semiformal high-level design | ADV_HLD.2 | PASS |
| Implementation of the TSF | ADV_IMP.1 | PASS |
| Descriptive low-level design | ADV_LLD.1 | PASS |
| Semiformal correspondence demonstration | ADV_RCR.1 | PASS |
| Formal TOE security policy model | ADV_SPM.1 | PASS |

| Assurance classes and components | | Verdict |
|---|---|---|
| Guidance documents | CC Class AGD | PASS |
| Administrator guidance | AGD_ADM.1 | PASS |
| User guidance | AGD_USR.1 | PASS |
| Life cycle support | CC Class ALC | PASS |
| Sufficiency of security measures | ALC_DVS.1 | PASS |
| Standardised life-cycle model | ALC_LCD.1 | PASS |
| Compliance with implementation standards | ALC_TAT.1 | PASS |
| Tests | CC Class ATE | PASS |
| Analysis of coverage | ATE_COV.2 | PASS |
| Testing: low-level design | ATE_DPT.1 | PASS |
| Functional testing | ATE_FUN.1 | PASS |
| Independent testing – sample | ATE_IND.2 | PASS |
| Vulnerability assessment | CC Class AVA | PASS |
| Analysis and testing for insecure states | AVA_MSU.3 | PASS |
| Strength of TOE security function evaluation | AVA_SOF.1 | PASS |
| Highly resistant | AVA_VLA.4 | PASS |

**Table 3: Verdicts for the assurance components**

The evaluation has shown that:

- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL4 augmented by AVA_VLA.4 and AVA_MSU.3

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2)

The results of the evaluation are only applicable to the S-TRUST Sign-it base components 2.0, Version 2.0.0.1 in the configuration defined in the Security Target [6] and summarised in this report (see chapter 2, chapter 4 and chapter 8).

The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

# 10 Comments/Recommendations

The User Guidance documentation (refer to chapter 6 of this report) contains important information about the secure usage of the TOE. Additionally, for secure usage of the TOE the fulfilment of the assumptions about the environment in the Security Target [6] and the Security Target as a whole has to be taken into account. Therefore a user has to follow the guidance in these documents.

As outlined in chapter 5 of this report and in the Security Target the TOE uses the hashfunctions SHA-1, SHA-256, SHA-384, SHA-512 and RIPEMD 160. For the verification of electronic signatures the TOE uses the RSA-Algorithms with 1024-2048 Bits.

According to the publication in the Bundesanzeiger Nr. 59, S. 4695-4696, these algorithms are considered to be suitable for the application of qualified electronic signatures with respect to the German Signature Law (SigG) and ordinance on electronic signatures.

As stated by the Bundesnetzagentur the hash functions SHA-1 and RIPEMD 160 are considered to be suitable for the application of qualified electronic signatures over the next six years, i.e. until end 2010. The hash functions SHA-256, SHA-384 and SHA-512 may be used to ensure an acceptable security level for a longer period  of time.

The RSA-Algorithm with 1024 Bits must not be used for the application of qualified electronic signatures after the end of 2007. A bitlength of 2048 Bits is still suitable after the end of 2010. Detailed information about the required bitlength for the validity of the RSA-Algorithm can be retrieved from the publications of the Bundesnetzagentur (see www.bundesnetzagentur.de).

# 11 Annexes

None.

# 12 Security Target

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

# 13 Definitions

## 13.1 Acronyms

| | |
|---|---|
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany |
| **CC** | Common Criteria for IT Security Evaluation |
| **CRL** | Certificate Revocation List |
| **EAL** | Evaluation Assurance Level |
| **IT** | Information Technology |
| **OSCP** | Online Certificate Status Protocol |
| **PP** | Protection Profile |
| **SF** | Security Function |
| **SFP** | Security Function Policy |
| **SOF** | Strength of Function |
| **ST** | Security Target |
| **TOE** | Target of Evaluation |
| **TSC** | TSF Scope of Control |
| **TSF** | TOE Security Functions |
| **TSP** | TOE Security Policy |

## 13.2 Glossary

**Augmentation** - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance 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 entity within the TSC that contains or receives information and upon which subjects perform operations.

**Protection Profile** - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

**Security Function** - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

**Security Target** - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

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

**Strength of Function** - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

**SOF-basic** - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

**SOF-medium** - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

**SOF-high** - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

**Subject** - An entity within the TSC that causes operations to be performed.

**Target of Evaluation** - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

**TOE Security Functions** - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

**TOE Security Policy** - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

**TSF Scope of Control** - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

# 14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999

[2] Common Methodology for Information Technology Security Evaluation (CEM), Part 1, Version 0.6; Part 2: Evaluation Methodology, Version 1.0, August 1999

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

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

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[6] Security Target BSI-DSZ-0314-2005 Version 3.3, 20.10.2005, Security Target (ST) Electronic Signature Application S-TRUST Sign-it base components 2.0, OPENLiMiT SignCubes AG

[7] Evaluation Technical Report, Version 1.0, 20.10.2005, Evaluation Technical Report BSI-DSZ-CC-0314, T-Systems GEI GmbH (confidential document)

[8] Configuration list, 20.10.2005, OPENLiMiT SignCubes AG

[9] User Guidance, Version 2.0.0.1, 20.10.2005, S-TRUST Sign-it 2.0 Benutzerdokumentation, OPENLiMiT SignCubes AG

[10] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG)1) vom 16. Mai 2001 (BGBl. I S. 876) zuletzt geändert durch Art. 1 des Ersten Gesetzes zur Änderung des Signaturgesetzes (1. SigÄndG), 04. Januar 2005, BGBl. Jahrgang 2005 Teil I S. 2

[11] Verordnung zur elektronischen Signatur (Signaturverordnung - SigV), 16.11.2001, BGBl. Jahrgang 2001 Teil I S. 876

[12] Maßnahmenkatalog für technische Komponenten nach dem Signaturgesetz, Stand 15. Juli 1998, Hrsg. RegTP

This page is intentionally left blank.

# C Excerpts from the Criteria

CC Part 1:

## **Caveats on evaluation results** (chapter 5.4) / **Final Interpretation 008**

The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to Part 2 (functional requirements), Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

**Part 2 conformant** - A PP or TOE is Part 2 conformant if the functional requirements are based only upon functional components in Part 2

**Part 2 extended** - A PP or TOE is Part 2 extended if the functional requirements include functional components not in Part 2

plus one of the following:

**Part 3 conformant** - A PP or TOE is Part 3 conformant if the assurance requirements are based only upon assurance components in Part 3

**Part 3 extended** - A PP or TOE is Part 3 extended if the assurance requirements include assurance requirements not in Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

***Package name* Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

***Package name* Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

***PP* Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.

CC Part 3:

## **Assurance categorisation** (chapter 2.5)

„The assurance classes, families, and the abbreviation for each family are shown in Table 2.1.

| Assurance Class | Assurance Family | Abbreviated Name |
|---|---|---|
| Class ACM: Configuration management | CM automation | ACM_AUT |
| | CM capabilities | ACM_CAP |
| | CM scope | ACM_SCP |
| Class ADO: Delivery and operation | Delivery | ADO_DEL |
| | Installation, generation and start-up | ADO_IGS |
| Class ADV: Development | Functional specification | ADV_FSP |
| | High-level design | ADV_HLD |
| | Implementation representation | ADV_IMP |
| | TSF internals | ADV_INT |
| | Low-level design | ADV_LLD |
| | Representation correspondence | ADV_RCR |
| | Security policy modeling | ADV_SPM |
| Class AGD: Guidance documents | Administrator guidance | AGD_ADM |
| | User guidance | AGD_USR |
| Class ALC: Life cycle support | Development security | ALC_DVS |
| | Flaw remediation | ALC_FLR |
| | Life cycle definition | ALC_LCD |
| | Tools and techniques | ALC_TAT |
| Class ATE: Tests | Coverage | ATE_COV |
| | Depth | ATE_DPT |
| | Functional tests | ATE_FUN |
| | Independent testing | ATE_IND |
| Class AVA: Vulnerability assessment | Covert channel analysis | AVA_CCA |
| | Misuse | AVA_MSU |
| | Strength of TOE security functions | AVA_SOF |
| | Vulnerability analysis | AVA_VLA |

**Table 2.1 -Assurance family breakdown and mapping“**

**Evaluation assurance levels** (chapter 6)

„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 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 6.1)

Table 6.1 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 2 of this 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 CC 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 extended with explicitly stated assurance requirements.

| Assurance Class | Assurance Family | Assurance Components by Evaluation Assurance Level | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | EAL1 | EAL2 | EAL3 | EAL4 | EAL5 | EAL6 | EAL7 |
| Configuration management | ACM_AUT | | | | 1 | 1 | 2 | 2 |
| | ACM_CAP | 1 | 2 | 3 | 4 | 4 | 5 | 5 |
| | ACM_SCP | | | 1 | 2 | 3 | 3 | 3 |
| Delivery and operation | ADO_DEL | | 1 | 1 | 2 | 2 | 2 | 3 |
| | ADO_IGS | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Development | ADV_FSP | 1 | 1 | 1 | 2 | 3 | 3 | 4 |
| | ADV_HLD | | 1 | 2 | 2 | 3 | 4 | 5 |
| | ADV_IMP | | | | 1 | 2 | 3 | 3 |
| | ADV_INT | | | | | 1 | 2 | 3 |
| | ADV_LLD | | | | 1 | 1 | 2 | 2 |
| | ADV_RCR | 1 | 1 | 1 | 1 | 2 | 2 | 3 |
| | ADV_SPM | | | | 1 | 3 | 3 | 3 |
| Guidance documents | AGD_ADM | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| | AGD_USR | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Life cycle support | ALC_DVS | | | 1 | 1 | 1 | 2 | 2 |
| | ALC_FLR | | | | | | | |
| | ALC_LCD | | | | 1 | 2 | 2 | 3 |
| | ALC_TAT | | | | 1 | 2 | 3 | 3 |
| Tests | ATE_COV | | 1 | 2 | 2 | 2 | 3 | 3 |
| | ATE_DPT | | | 1 | 1 | 2 | 2 | 3 |
| | ATE_FUN | | 1 | 1 | 1 | 1 | 2 | 2 |
| | ATE_IND | 1 | 2 | 2 | 2 | 2 | 2 | 3 |
| Vulnerability assessment | AVA_CCA | | | | | 1 | 2 | 2 |
| | AVA_MSU | | | 1 | 2 | 2 | 3 | 3 |
| | AVA_SOF | | 1 | 1 | 1 | 1 | 1 | 1 |
| | AVA_VLA | | 1 | 1 | 2 | 3 | 4 | 4 |

**Table 6.1 - Evaluation assurance level summary“**

### **Evaluation assurance level 1 (EAL1) - functionally tested** (chapter 6.2.1)

„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 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, and that it provides useful protection against identified threats.“

### **Evaluation assurance level 2 (EAL2) - structurally tested** (chapter 6.2.2)

„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 practice. 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 6.2.3)

„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 practices.

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 6.2.4)

„Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices 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 6.2.5)

„Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices 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 6.2.6)

„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 6.2.7)

„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.“

## **Strength of TOE security functions (AVA_SOF)** (chapter 14.3)

**AVA_SOF** Strength of TOE security functions

„Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.“

## **Vulnerability analysis (AVA_VLA)** (chapter 14.4)

**AVA_VLA** Vulnerability analysis

„Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.“

„Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.“

„Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2), moderate (for AVA_VLA.3) or high (for AVA_VLA.4) attack potential.“

This page is intentionally left blank.