BSI-DSZ-CC-0508-2008

for

S-TRUST Sign-it Basiskomponenten 2.1,
Version 2.1.7.1

from

OPENLiMiT SignCubes AG

Deutsches **IT-Sicherheitszertifikat**
erteilt vom   Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0508-2008

Signaturanwendungskomponente

S-TRUST Sign-it Basiskomponenten 2.1
Version 2.1.7.1

from	**OPENLiMiT SignCubes AG**
Functionality:	**Product specific Security Target** **Common Criteria Part 2 extended**
Assurance:	**Common Criteria Part 3 conformant** **EAL4 augmented by** **AVA_MSU.3 – Analysis and testing for insecure** **states AVA_VLA.4 – Highly resistant**

Common Criteria
Arrangement
for components up
to EAL 4

Common Criteria

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, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 augmented and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

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, 26 June 2008
For the Federal Office for Information Security

Irmela Ruhrmann   L.S.
Head of Division

IT
Security
Certified

SOGIS - MRA

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 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) [3]

- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5]

- Common Methodology for IT Security Evaluation, Version 2.3

- BSI certification: Application Notes and Interpretation of the Scheme (AIS)

- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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

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). The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

---

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 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 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

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

2.2 International Recognition of 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 has been signed in May 2000 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC.

As of February 2007 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, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

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 Basiskomponenten 2.1, Version 2.1.7.1 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0494-2007.

The evaluation of the product S-TRUST Sign-it Basiskomponenten 2.1, Version 2.1.7.1 was conducted by T-Systems GEI GmbH. The evaluation was completed on 13. May 2008. The T-Systems GEI GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: OPENLiMiT SignCubes AG

The product was developed by: OPENLiMiT SignCubes AG

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

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, where specified in the following report and in the Security Target.

---

[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.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular 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 S-TRUST Sign-it Basiskomponenten 2.1, Version 2.1.7.1 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://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]   OPENLiMiT SignCubes AG
       Zugerstrasse 76B
       CH 6341 Baar
       Schweiz

B Certification Results

The following results represent a summary of

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

1 Executive Summary

The Target of Evaluation (TOE) and subject of the Security Target (ST) is the software application S-TRUST Sign-it Basiskomponenten 2.1, Version 2.1.7.1[8].

S-TRUST Sign-it Basiskomponenten 2.1, Version 2.1.7.1 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.

The S-TRUST Sign-it Basiskomponenten 2.1 were developed for the use on the operating systems from Microsoft since Microsoft Windows NT 4.0. 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 provides 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 the RSA-Algorithm for signature validation. It 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 can be used as a standalone application or can be integrated into third party products. For third party products the TOE includes an API (called OPENLiMiT SignCubes Job Interface or OPENLiMiT SignCubes SDK v2.1) that allows access to the following core functionality of the TOE:

● Computation of hash values implementing the algorithms mentioned above.

● Creation of electronic signatures.

● Timestamp processing.

● Support for attribute certificates in the process of electronic signature creation.

● Support for OCSP-processing in the process of electronic signature creation.

● Electronic signature verification.

● Integrity protection of the installed product.

Furthermore, 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 in order to ensure that the user is assured about the content to be signed or the content of the signed file.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

---

[8]   Also named S-TRUST Sign-it Basiskomponenten 2.1 in this report.

[9]   see [11]

[10]   see [12]

The TOE security assurance requirements 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 AVA_MSU.3 and AVA_VLA.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target [6], chapter 5.3.

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

TOE Security Function	Addressed issue
SF.1	Hash value computation and initiation of the electronic signature creation process using certificates, smart card terminals and secure signature creation devices. The user can optionally include OCSP-responses for the validation of certificates and add timestamps to a digital signature. Furthermore, the S-TRUST Sign-it Basiskomponenten 2.1 allow the creation of more than one signature without entering the PIN for every document[11]. This feature is only available for the OPENLiMiT SignCubes Job Interface and not for the graphical user interface included in the S-TRUST Sign-it Basiskomponenten 2.1.
SF.2	Verification of hash values and electronic signatures using certificate revocation lists, OCSP responses (optional) and timestamps (optional) Apart from the extraction of the original and the comparison with the calculated hash value the S-TRUST Sign-it Basiskomponenten 2.1 verify the certificate chain using the chain model or RFC 3280.
SF.3	Program module manipulation detection The files and libraries constituting the S-TRUST Sign-it Basiskomponenten 2.1 are digitally signed. Each time the application starts a specific module is responsible for verfying these signatures mathematically.
SF.4	Unambiguous presentation of the data to be signed The S-TRUST Sign-it Basiskomponenten 2.1 present the data to be signed unambigiously to the user. To accomplish this, a parser determines whether the format of the data to be signed complies to the Adobe PDF-, the TIFF-standard or is a text file. The data is checked for active content, unknown tags and elements or control characters that cannot be displayed. If any irregularities are detected, the user is informed with appropriate error messages or warnings.
SF.5	Protection against hash value manipulation Before the electronic signature is initiated, the S-TRUST Sign-it

---

[11]   Though the software provides this functionality, the supported smart cards require entering the PIN for every document.

TOE Security Function	Addressed issue
	Basiskomponenten 2.1 compute the hash value of the data to be signed. After the electronic signature creation process the S-TRUST Sign-it Basiskomponenten 2.1 verifiy 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 signature is discarded.
SF.6	Assurance of the TOE's integrity

For the integrity check the S-TRUST Sign-it Basiskomponenten 2.1 comprise a JAVA-applet that is provided online. When assessing this applet it calculates the hash value of each file belonging to the S-TRUST Sign-it Basiskomponenten 2.1 and compares it to the values that were initially caluculated by the manufacturer. If any value does not match, an error message is displayed. |
| SF.7 | Processing of OCSP information for certificate validation

The S-TRUST Sign-it Basiskomponenten 2.1 is able to process OCSP-responses. First the mathematical correctness of the signature of the OCSP-response is checked. If the OCSP-response is used for the validation of a certificate, the complete chain for the signing certificate of the OCSP-response is verified. |
| SF.8 | Application of Timestamps

The S-TRUST Sign-it Basiskomponenten 2.1 apply timestamps to files if the timestamp is electronically signed and the certificate belonging to the signature of the timestamp is already available. Otherwise the timestamp is not imported. |
| SF.9 | Validation of Timestamps

The S-TRUST Sign-it Basiskomponenten 2.1 validate the electronic signature of a timestamp mathematically. Furthermore, the certificate underlying the electronic signature of the timestamp is validated according to the chain model or RFC 3280. A prerequisite for this security function is that the signing certificate of the timestamp is already available. |
| SF.10 | Management of Security Functions depending on licenses

The S-TRUST Sign-it Basiskomponenten 2.1 support different licenses. E.g. for the verification of electronic signatures no special license key must be purchased, whereas the creation of embedded PDF-signatures requires the availability of the most comprehensive license |

Table 1: Security Functions

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

The claimed TOE's strength of functions high (SOF-high) for specific functions as indicated in the Security Target [6], chapter 8 is confirmed. 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). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 4. Based on these assets the security environment is defined in terms of assumptions, threats and policies. This is outlined in the Security Target [6], chapter 3.

This certification covers the following configurations of the TOE: The TOE is a software application that does not require a special configuration. The TOE has to be configured in accordance with the Security Target and the respective guidance documents. This means among other aspects that for the application of qualified electronic signatures a smartcard reader and a secure signature creation device must be used that was approved in accordance with the German signature law [11]. The Security Target names the products the TOE can be used with.

Further information about the configuration of the TOE and the technical environment is available in

- the Security Target [6],

- chapter 1, chapter 4 and chapter 8 of this report,

- the user guidance [9],

- and the guidance of the API provided by the TOE [9].

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:

S-TRUST Sign-it Basiskomponenten 2.1, Version 2.1.7.1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Date	Form of Delivery
1.	SW (program)	S-TRUST Sign-it base components 2.1, version 2.1.7.1	2.1.7.1	19.03.2008	File
2.	DOC	S-TRUST Sign-it Basiskomponenten 2.1, Version 2.1.7.1 – User Guidance (German)	2.1.7.1	27.02.2008	chm-File
3.	DOC	OPENLiMiT® SignCubes SDK v2.1 Documentation	1.2	05.03.2007	PDF-File
4.	Header File	siqSDK.h		21.01.2008	File
5.	Library File	siqSDK.lib		05.12.2007	File
6.	DOC	Developer Documentation OPENLiMiT® SignCubes SDK	1.7	28.01.2008	PDF-File
7.	Header File	siqVendor.h		21.01.2008	File

No	Type	Identifier	Release	Date	Form of Delivery
8.	Integrity-Tool	IntegrityTool.jar		12.12.2007	File

Table 2: Deliverables of the TOE

The TOE deliverables No.1 to No.2 are provided for a standard customer, who purchases the TOE.

The TOE deliverables No.3 to 5 are delivered additionally and have to be purchased separately. The TOE deliverables No.6 and No.7 can be used internally by the developer of the TOE. The TOE deliverable No.8 is used to verify the integrity of the TOE.

To identify the Header, Library and Jar Files the SHA-1 values of these files are listed in the table 3.

No.	File	SHA-1-value
1.	siqSDK.h	9eae545de45ec0bb05284e62169396d8876ee8ed
2.	siqVendor.h	b449d1302fdf1aa211efb7f7decf6ac9ce8e6ba5
3.	siqSDK.lib	c9f82151769caf7552c1a85acaf988da59d794e4
4.	IntegrityTool.jar	b681b7e30b5141db02c7c4e783fbf4d52a0f3a3b

Table 3: Hash Values of TOE deliverables

The vendor provides the product either as a complete setup that comprises the user guidance in both languages and supports all smart cards as well as all smart card terminals that are listed in chapter 4.

Alternatively, the TOE is distributed in different parts comprising the compulsory minimal setup and optional add-on setups.

The minimal setup contains the following constituent parts of the evaluated product:

● the user guidance and user prompting either in English or in German,

● all binary files with exception of the ones that are required for the support of the smart cards and smart card terminals listed in chapter 4 and

● especially the S-TRUST Sign-it Integrity Tool.

After the installation of the minimal setup all functionalities of the product are available that the most restrictive license allows to use.

The add-on setups are composed according to the needs of the customer and contain the libraries required to support specific smart cards and smart card terminals. To use the functionalties of other licenses of the product than the most restrictive one the installation of the corresponding add-on setup in addition to the installation of the minimal setup is required.

As a third alternative the vendor provides single setups that contain the minimal setup and the support for a selected set of smart cards and smart card terminals. This alternative may be chosen to provide a software package for a set of hardware that a Trust Center or a major reseller dispenses.

The end-customer can acquire the TOE through different sales channels:

- The costumer buys a CD-ROM that contains the required setup directly from OPENLiMiT SignCubes AG or resellers.

- Resellers or the OPENLiMiT SignCubes AG make the software available on their webpages. The download process must comply to the following guidelines:

  - The webpage where the software is offered must be secured by means of https. The fingerprint of the certificate must be published separately on the website of the corresponding company.

  - The website must explicitly instruct the user to execute the integrity tool first before using the TOE.

After installing the product the user is compelled to execute the S-TRUST Sign-it Integrity Tool. This applet is provided by OPENLiMiT SignCubes AG on the website

https://www.openlimit.com/integritytool

The S-TRUST Sign-it Integrity Tool checks whether the TOE is correctly installed on the computer of the user and displays the versions of the different files composing the TOE. Thus, the user can easily recognize whether he installed the correct version of the software and which parts of the evaluated product are installed.

The TOE deliverables No. 3 to No. 5 can only be acquired from OPENLiMiT SignCubes AG. They are handed over to end customers (i.e. application developers) either online or by a delivery service on CD-ROM as a compressed zip-archive. The archive is digitally signed with a qualified electronic signature. The belonging qualified certificate can be identified by means of the following information:

Subject:	Armin Lunkeit
Issuer:	S-TRUST Qualified Signature CA 2005-001:PN
Valid From:	11th of October 2005
Valid Until:	31 of December 2009
Serial Number:	0x6A 41 76 EC AB 31 41 3B DC B3 87 A0 2A 62 E6 BF
SHA-1 Fingerprint:	49 DA 34 B5 BF C2 8A 41 38 1D 52 2C 6E C6 24 BD C3 0E 08 38

The receiver of the archive must verify this qualified electronic signatur to ensure the integrity and authenticity of the software.

3 Security Policy

The S-TRUST Sign-it Basiskomponenten 2.1, Version 2.1.7.1 is a signature application component compliant to the German signature law and ordinance on electronic signature and thus enforces the following security policies:

- The TOE clearly indicates the creation of a qualified electronic signature and enables the user to unambigiously identify the data to be signed.

- 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 is 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 nonreadable 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

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:

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 installed TOE as described in the user documentation and on the website where from the different setups can be downloaded.

Environmental assumptions

- **A.Platform**

  The user utilizes an Intel 586 compatible computer as hardware platform, which contains at least 64 MB of RAM and 120 MB of free disk space. On the computer one of the following operating systems is installed:

    - Windows NT 4.0 SP 6

    - Windows 2000 SP 2

    - Windows 2003

    - Windows XP Home

    - Windows XP Professional

    - Windows XP Tablet PC Edition

    - Windows XP 64 Bit Edition

    - Windows Vista

    - Windows Vista 64 Bit Edition

Additionally the TOE supports a terminal server environment under Windows operating systems Windows 2000 with Citrix Metaframe and Windows 2003 with and without Citrix Metaframe.

In a terminal server environment the communication between server and client/s is conducted via an encrypted channel and is therefore to be considered trustworthy.

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[12].

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.

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
- ZKA Banking signature card, v6.2 NP, Type 3 from Giesecke & Devrient
- ZKA Banking signature card v6.31 NP, Type 3 from Giesecke & Devrient
- ZKA Banking signature card v6.32, Type 3 from Giesecke & Devrient
- ZKA Banking Signature Card, Version 6.4 from Giesecke & Devrient
- ZKA Banking Signature Card, Version 6.51 from Giesecke & Devrient
- ZKA Banking Signature Card, v6.6 from Giesecke & Devrient
- ZKA signature card, version 5.02 from Gemplus-mids GmbH
- ZKA signature card, version 5.10 (ZKA 680 V5A) from Gemplus-mids GmbH
- ZKA signature card, version 5.11 from Gemplus-mids GmbH
- ZKA signature card, version 5.11 M from Gemplus GmbH (Gemalto)
- ZKA SECCOS Sig v1.5.3 from Sagem Orga GmbH

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 ST-2000
- Kobil B1 Pro USB
- Kobil TriB@nk
- Kobil KAAN Advanced
- SCM Microsystems SPRx32

---

[12]   The manual installation of the Microsoft SmartCard base components is required for Microsoft Windows NT 4.0, SP 6

- Reiner SCT cyberJack e-com v2.0

- Reiner SCT cyberJack e-com v3.0

- Reiner SCT cyberJack pinpad v2.0

- Reiner SCT cyberJack pinpad v3.0

- Omnikey Cardman 3621

- Omnikey Cardman 3821

- Fujitsu Siemens S26381-K329-V2xx HOS:01

The used components are approved components according to the German signature law. The certificates can be obtained from the BSI (www.bsi.bund.de).

- **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.

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.

Restrictions and Exceptions

The following tables show the combinations between operating system, smart card and smart card reader that are not supported.

Table 4 depicts which smart card terminals are not supported by the corresponding operating system.

Operating system	Smart card terminal
Windows NT 4 SP 6	Cherry St 2000 (Firmware version 5.08)
	Cherry ST2000 (Firmware version 5.11)
	Reiner SCT cyberJack pinpad v3.0
	Reiner SCT cyberJack e-com v3.0
	Kobil KAAN Advanced
	Kobil TriB@nk
	Kobil B1 Pro USB
	Fujitsu Siemens S26381-K329-V2xx HOS: 01
	Omnikey Cardman 3621
	Omnikey Cardman 3821
Windows XP 64 Bit Edition	Kobil KAAN Advanced
	Kobil TriB@nk
	Kobil B1 Pro USB
	SCM SPRx32 (Firmware version 4.15)
	SCM SPR x32 (Firmware version 5.10)
Windows Vista	Reiner SCT cyberJack pinpad v2.0
	Reiner SCT cyberJack e-com v2.0
	SCM SPRx32 (Firmware version 4.15)
Windows Vista 64 Bit Edition	Kobil KAAN Advanced
	Kobil B1 Pro USB
	Kobil TriB@nk
	SCM SPRx32 (Firmware version 4.15)
	SCM SPR x32 (Firmware version 5.10)
	Reiner SCT cyberJack pinpad v2.0
	Reiner SCT cyberJack e-com v2.0
Windows 2000 Server with Citrix Meta Frame	Kobil TriB@nk
	Kobil B1 Pro USB
Windows 2003 Server with Citrix Meta Frame	Kobil TriB@nk

Table 4: Incompatibility between operating system and smart card terminals

These combinations are not included in the evaluation and therefore not included in the certificate.

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

5 Architectural Information

The TOE S-TRUST Sign-it Basiskomponenten 2.1, Version 2.1.7.1 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 the   may be used as a single application but also may be integrated into third party products. 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 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 overview of the main components and their interfaces as described in the High-Level Design.
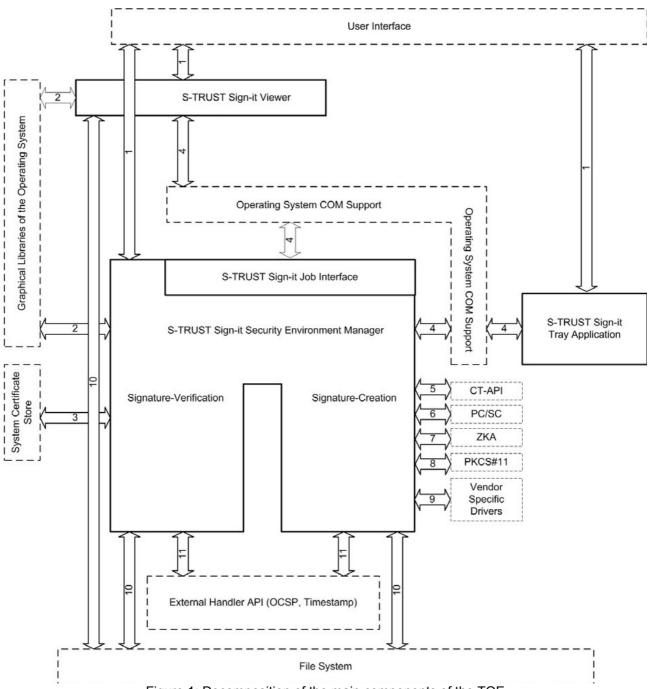
Figure 1: Decomposition of the main components of the TOE

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 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 1.7 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 SDK:

● 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 (smart card reader).

● 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 S-Trust Sign-it base components installed on the user's computer.

Providing graphical interfaces in the process of signature creation, verification and product configuration

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

Developer tests

The tests of the developer were conducted with the smard cards, smart card terminals and operating systems listed in chapter 4 assumption A.Platform and thus in accordance with the ST [6]. All additional prerequisites mentioned in the assumptions on the operating environment (see chapter 1 and chapter 4 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.

All tests of the developer were conducted with the same version of the TOE that is listed in the configuration list [8]. The test description demonstrates that the developer performed his testing on an adequate level for the evaluation assurance level EAL4+. 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.

Evaluator tests

Due to the evaluation assurance level EAL 4+ the ITSEF is obliged to repeat a subset of the developer tests as well as conduct independent and penetration tests to a commensurate extent.

For the repetition of the developer tests the testbed of the developer was used. The independent evaluator tests follow two different test approaches. On the one hand tests are derived from the developer tests to examine the behaviour of the TOE in a broader approach. This kind of tests strengthen the confidence of the evaluators in the test approach of the developer. On the other hand the evaluators developed new tests to examine special reactions of the TOE. Due to this probing the existence of certain vulnerabilities can be eleminated.

For the evaluator tests at the ITSEF facility in Bonn the following configuration was employed:

- Computer with Windows 2000, Service Pack 4 and JRE 1.4.2_08

- Card reader SCM Microsystems SPR x32

- Smart card ZKA Banking signature card, v6.2b NP and 6.2f NP, Type 3 from Giesecke & Devrient

Test results

The tests showed that the TOE behaves as expected. The depth of testing is adequate for the evaluation assurance level chosen EAL 4+. The TOE successfully passed independent testing. The tests performed by the evaluators confirmed that under the given assumptions no vulnerabilities can be exploited.

8 Evaluated Configuration

The TOE was evaluated in the configuration as described in the Evaluation Technical Report [7] and summarized in chapter 2 of this report.

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

9.1 CC specific results

The Evaluation Technical Report (ETR), [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The evaluation methodology CEM [2] was used for those components used up to EAL4 extended by advice of the Certification Body for components beyond EAL 4 augmented and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

i)   *Anwendungshinweise und Interpretationen zum Schema, AIS20, Version 1, 02.12.1999, Bundesamt für Sicherheit in der Informationstechnik (BSI), Bonn, Ein Vorschlag zu: Funktionsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren*
(see [4], AIS 20) were used.

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

● All components of the class ASE

● All components of the EAL 4 augmented package as defined in the CC (see also part C of this report)

● The components
AVA_MSU.3 – Analysis and testing for insecure states

● AVA_VLA.4 – Highly resistant
augmented for this TOE evaluation.

● All components claimed in the Security Target [6], chapter 5.2 and defined in the CC (see also part C of this report).

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0494-2008, re-use of specific evaluation tasks was possible.

The evaluation has confirmed:

● for the functionality: Product specific Security Target
                            Common Criteria Part 2 extended

● for the assurance: Common Criteria Part 3 conformant
                            EAL4 augmented by
                            AVA_MSU.3 – Analysis and testing for insecure states
                            AVA_VLA.4 – Highly resistant

The following TOE Security Functions fulfil the claimed Strength of Function high:
(i)   the TOE Security Function

● SF.1 (Hash value computation and initiation of the electronic signature creation)

● SF.2 (Verification of hash values and electronic signatures)

● SF.3 (Program module manipulation detection)

● 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)

(ii)   and for other usage of encryption and decryption within the TOE.

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 TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2 Results of cryptographic assessment

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 holds for:

● the TOE Security Function SF.1 and

● SF.2.

The following cryptographic algorithms are used by the TOE to enforce its security policy:

– hash functions:

– SHA-1, SHA-256, SHA-384, SHA-512 and RIPEMD 160

– algorithms for the encryption and decryption:

  RSA-Algorithms with bitlengths between 1024-2048 bits.

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 4, Para. 3, Clause 2). According to Bundesnetzagentur – Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), vom 17.12.2007 the algorithms are suitable for - Erzeugung und Prüfung von qualifizierten elektronischen Signaturen -.

The following table describes the validity period of hash functions according to the publication of the Bundesnetzagentur [14].

Hash function	Valid until end of
SHA-1	June 2008
RIPEMD 160	2010
SHA-256, SHA-384, SHA-512	2014

Table 8: Validity period of hash functions

As the S-TRUST Sign-it Basiskomponenten 2.1, Version 2.1.7.1 implement certain cryptographic algorithms for the verification of electronic signatures, the following table summarizes the validity period of these algorithms as published by the Bundesnetzagentur.

Algorithm with bitlength	Valid until end of
RSA 1024	2007
RSA 1280	2008
RSA 1536	2009
RSA 1728	2010
RSA 1976	2014

Table 9: Validity period of cryptographic algorithms

A bitlength of 2048 Bits is recommended for an acceptable long term security level.

Detailed information about suitable algorithms for the application of qualified electronic signatures can be obtained from the website of the Bundesnetzagentur (see www.bundesnetzagentur.de).

10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered.

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

API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
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

12.2 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.

13 Bibliography

[1]   Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2]   Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

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

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

specifically:

-       AIS 25, Version 3, 6 August 2007 for: CC Supporting Document, - The Application of CC to Integrated Circuits, Version 2.0, CCDB-2006-04-003, April 2006

-       AIS 26, Version 3, 6 August 2007 for: CC Supporting Document, -Application of Attack Potential to Smartcards, Version 2.3, CCDB-2007-04-001, April 2007

-       AIS 31, Version 1, 25 Sept. 2001 for: Functionality classes and evaluation methodology of physical random number generators

-       AIS 32, Version 1, 02 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungs-schema.

-       AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+

-       AIS 35 ST-lite

-       AIS 36, Version 1, 29 July 2002 for: CC Supporting Document, ETR-lite for Composition, Version 1.1, July 2002 and CC Supporting Document, ETR-lite for Composition: Annex A Composite smartcard evaluation, Version 1.2 March 2002

-       AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

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

[6]   Security Target BSI-DSZ-0508-2008, Version 1.4, 18.03.2008, Electronic Signature Application S-TRUST Sign-it Basiskomponenten 2.1, Version 2.1.7.1, OPENLiMiT SignCubes AG

[7]   Evaluation Technical Report, Version 1.0, 08.04.2008, T-Systems GEI GmbH (confidential document)

[8]   Configuration list for the S-TRUST Sign-it Basiskomponenten 2.1, Version 2.1.7.1, 04.04.2008, OPENLiMiT SignCubes GmbH (confidential document)

Guidance documentation

[9]   S-TRUST Sign-it Basiskomponenten 2.1, Version 2.1.7.1, User Guidance, Version 2.1.7.1, OPENLiMiT SignCubes GmbH, file: deuS-TRUST Sign-it. chm, 3.184.117 bytes, 27.02.2008.

OPENLiMiT SignCubes SDK v2.1, Release 1.2, 05.03.2007, OPENLiMiT SignCubes GmbH

[10] Auslieferungshinweise für Terminalserverlizenzen, S-TRUST Sign-it Basiskomponenten 2.1, Version 2.1.7.1, Version 1.0, OPENLiMiT SignCubes GmbH

Legal regulations

[11] 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), 01/04/2005, BGBl. volume 2005 part I p. 2

[12] Verordnung zur elektronischen Signatur (Signaturverordnung - SigV), 11/16/2001, BGBl. volume 2001 part I p. 876

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

[14] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), published February 05, 2008, in the Bundesanzeiger No. 19, p. 376 and available on the web-pages of the Bundesnetzagentur).

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„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 CC Part 2 (functional requirements), CC 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:

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

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

plus one of the following:

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

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

Protection Profile criteria overview (chapter 8.2)

"The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry."

"Assurance Class	Assurance Family
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements "

Security Target criteria overview (Chapter 8.3)

"The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation."

"Assurance Class	Assurance Family
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements "

Assurance categorisation (chapter 7.5)

"The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
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)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping"

Evaluation assurance levels (chapter 11)

"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 11.1)

"Table 6 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 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 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: Evaluation assurance level summary"

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

"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 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 11.4)

"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 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 11.5)

"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 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 11.6)

"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 11.7)

"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 11.8)

"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 11.9)

"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."

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

"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 19.4)

"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 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential."

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.