



# Certification Report

**Bundesamt für Sicherheit in der Informationstechnik**

**BSI-DSZ-CC-0432-2007**

for

**OPENLiMiT SignCubes base components 2.1  
Version 2.1.6.1**

from

**OPENLiMiT SignCubes AG**

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn  
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111



# Deutsches IT-Sicherheitszertifikat

erteilt vom  
Bundesamt für Sicherheit in der Informationstechnik



Bundesamt für Sicherheit  
in der Informationstechnik

**BSI-DSZ-CC-0432-2007**

**Signature application component**

**OPENLiMiT SignCubes base components 2.1  
Version 2.1.6.1**

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, version 2.3* (ISO/IEC 15408:2005) extended by advice of the Certification Body for components beyond EAL4 for conformance to the *Common Criteria for IT Security Evaluation, version 2.3* (ISO/IEC 15408:2005).

### **Evaluation Results:**

Functionality: **Product specific Security Target  
Common Criteria Part 2 extended**

Assurance Package: **Common Criteria Part 3 conformant  
EAL4 augmented by  
AVA\_MSU.3 – Analysis and testing for insecure states  
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, May 16<sup>th</sup> 2007

The President of the Federal Office  
for Information Security



SOGIS - MRA

Dr. Helmbrecht

L.S.

**Bundesamt für Sicherheit in der Informationstechnik**

Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn  
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSI-G 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<sup>1</sup> 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.

---

<sup>1</sup> Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

## **Contents**

Part A: Certification

Part B: Certification Results

Part C: Excerpts from the Criteria

## A Certification

### 1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG<sup>2</sup>
- BSI Certification Ordinance<sup>3</sup>
- BSI Schedule of Costs<sup>4</sup>
- 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 2.3<sup>5</sup>
- Common Methodology for IT Security Evaluation (CEM), 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)

---

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

<sup>3</sup> 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

<sup>4</sup> 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

<sup>5</sup> Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

## **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 in March 1998. This agreement has been 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) recognizes certificates issued by the national certification bodies of France and the United Kingdom within 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>

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 OPENLiMiT SignCubes base components 2.1, Version 2.1.6.1 has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0423-2007

The evaluation of the product OPENLiMiT SignCubes base components 2.1, Version 2.1.6.1 was conducted by T-Systems GEI GmbH. The T-Systems GEI GmbH is an evaluation facility (ITSEF)<sup>6</sup> recognised by BSI.

The sponsor, vendor and distributor is:

OPENLiMiT SignCubes AG  
Zugerstrasse 76 B  
6341 Baar  
Switzerland

The certification is concluded with

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

This work was completed by the BSI on 16. May 2007.

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.

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.

---

<sup>6</sup> Information Technology Security Evaluation Facility

## 4 Publication

The following Certification Results contain pages B-1 to B-30.

The product OPENLiMiT SignCubes base components 2.1, Version 2.1.6.1 has been included in the BSI list of the certified products, which is published regularly (see also Internet: [http:// www.bsi.bund.de](http://www.bsi.bund.de)). Further information can be obtained from BSI-Infoline +49 3018 9582-111.

Further copies of this Certification Report can be requested from the vendor<sup>7</sup> of the product. The Certification Report can also be downloaded from the above-mentioned website.

---

<sup>7</sup> OPENLiMiT SignCubes AG  
Zugerstrasse 76 B  
6341 Baar  
Switzerland

## **B Certification Results**

The following results represent a summary of

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

## Contents of the certification results

1	Executive Summary	3
2	Identification of the TOE	9
3	Security Policy	12
4	Assumptions and Clarification of Scope	12
5	Architectural Information	19
6	Documentation	21
7	IT Product Testing	22
8	Evaluated Configuration	23
9	Results of the Evaluation	23
10	Comments/Recommendations	25
11	Annexes	26
12	Security Target	26
13	Definitions	27
14	Bibliography	29

## 1 Executive Summary

The Target of Evaluation (TOE) and subject of the Security Target (ST) is the software application OPENLiMiT SignCubes base components 2.1, Version 2.1.6.1<sup>8</sup>.

OPENLiMiT SignCubes base components 2.1 is an electronic signature application compliant to the German electronic signature law<sup>9</sup> and ordinance on electronic signatures<sup>10</sup>. The application itself is a set of executables and programming libraries.

The OPENLiMiT SignCubes base components 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.

---

<sup>8</sup> Also named OPENLiMiT SignCubes base components 2.1 in this report.

<sup>9</sup> see [12]

<sup>10</sup> see [13]

Furthermore, the TOE provides a legal binding displaying unit (OPENLiMiT SignCubes 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 IT product OPENLiMiT SignCubes base components 2.1, Version 2.1.6.1 was evaluated by T-Systems GEI GmbH. The evaluation was completed on 25. April 2007. The T-Systems GEI GmbH is an evaluation facility (ITSEF)<sup>11</sup> recognised by BSI.

The sponsor, vendor and distributor is:

OPENLiMiT SignCubes AG  
 Zugerstrasse 76 B  
 6341 Baar  
 Switzerland

### 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 Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL4 (Evaluation Assurance Level 4 augmented). The following table shows the augmented assurance components.

Requirement	Identifier
EAL4	TOE evaluation: methodically designed, tested, and reviewed
+: AVA_MSU.3	Analysis and testing for insecure states
+: AVA_VLA.4	Highly resistant

Table 1: Assurance components and EAL-augmentation

### 1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 extended as shown in the following tables.

The following SFRs are taken from CC part 2:

Security Functional Requirement	Addressed issue
<b>FCS</b>	Cryptographic support
FCS_COP.1	Cryptographic operation,
<b>FDP</b>	User data protection
FDP_DAU.2	Data authentication with identity of guarantor

<sup>11</sup> Information Technology Security Evaluation Facility

Security Functional Requirement	Addressed issue
FDP_ITC.1	Import of user data without security attributes
<b>FMT</b>	Security management
FMT_MOF.1	Management of security functions behaviour
FMT_SMF.1	Specification of management functions
<b>FTP</b>	Protection of the TOE Security Functions
FTP_ITC.1	Inter-TSF trusted channel

Table 2: SFRs for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined:

Security Functional Requirement	Addressed issue
FDP_SVR.1	Secure Viewer

Table 3: SFRs for the TOE, CC part 2 extended

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST [6], chapter 5.1.

The following Security Functional Requirements are defined for the IT-Environment of the TOE:

Security Functional Requirement	Addressed issue
FCS_COP.1	Cryptographic operation,

Table 4: SFRs for the IT-Environment

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST, chapter 5.3.

These Security Functional Requirements are implemented by the TOE Security Functions:

TOE Security Function	Addressed issue
SF.1	<p>Hash value computation and initiation of the electronic signature creation process using certificates, smart card terminals and secure signature creation devices.</p> <p>The user can optionally include OCSP-responses for the validation of certificates and add timestamps to a digital signature. Furthermore, the OPENLiMiT SignCubes base components 2.1 allow the creation of more than one signature without entering the PIN for every document<sup>12</sup>. This feature is only available for the OPENLiMiT SignCubes Job Interface and not for the graphical</p>

<sup>12</sup> Though the software provides this functionality, the supported smart cards require entering the PIN for every document.

TOE Security Function	Addressed issue
	user interface included in the OPENLiMiT SignCubes base components 2.1.
SF.2	<p>Verification of hash values and electronic signatures using certificate revocation lists, OCSP responses (optional) and timestamps (optional)</p> <p>Apart from the extraction of the original and the comparison with the calculated hash value the OPENLiMiT SignCubes base components 2.1 verify the certificate chain using the chain model or RFC 3280.</p>
SF.3	<p>Program module manipulation detection</p> <p>The files and libraries constituting the OPENLiMiT SignCubes base components 2.1 are digitally signed. Each time the application starts a specific module is responsible for verifying these signatures mathematically.</p>
SF.4	<p>Unambiguous presentation of the data to be signed</p> <p>The OPENLiMiT SignCubes base components 2.1 present the data to be signed unambiguously 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.</p>
SF.5	<p>Protection against hash value manipulation</p> <p>Before the electronic signature is initiated, the OPENLiMiT SignCubes base components 2.1 compute the hash value of the data to be signed. After the electronic signature creation process the OPENLiMiT SignCubes base components 2.1 verify 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.</p>
SF.6	<p>Assurance of the TOE's integrity</p> <p>For the integrity check the OPENLiMiT SignCubes base components 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 OPENLiMiT SignCubes base components 2.1 and compares it to the values that were initially calculated by the manufacturer. If any value does not match, an error message is displayed.</p>
SF.7	<p>Processing of OCSP information for certificate validation</p> <p>The OPENLiMiT SignCubes base components 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.</p>

TOE Security Function	Addressed issue
SF.8	<p>Application of Timestamps</p> <p>The OPENLiMiT SignCubes base components 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.</p>
SF.9	<p>Validation of Timestamps</p> <p>The OPENLiMiT SignCubes base components 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.</p>
SF.10	<p>Management of Security Functions depending on licenses</p> <p>The OPENLiMiT SignCubes base components 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</p>

Table 5: Security Functions

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

### 1.3 Strength of Function

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

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.

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

The threats which were assumed for the evaluation and averted by the TOE are specified in the Security Target [6] and can be summarised as follows.

It is assumed that the attacker is a human being with high attack potential or a process acting on behalf of him.

The objects that must be protected are

- the document that should be signed
- a signature that must be verified
- the files and libraries the TOE consists of.

The following threats to these assets were identified in the Security Target:

- Manipulation of a user file
- Manipulation of a signed file
- Manipulation of the TOE and of its files
- Manipulation of a file before the users decision to sign the file
- Creation of a falsified electronic signature
- Downgrading of TOE's manageable capabilities.

The Security Target does not contain any organisational security policies.

### **1.5 Special configuration requirements**

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 [12]. 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 1.6, chapter 4.2 and chapter 8 of this report,
- the user guidance [9],
- and the guidance of the API provided by the TOE [11].

### **1.6 Assumptions about the operating environment**

For a secure operation of the TOE the following assumptions must be taken into account:

- The product must be installed on an Intel 586 compatible computer with 64 MB RAM and 60 MB free hard disk capacities.
- A Microsoft Windows operating system from Windows NT 4.0 onwards must be installed.
- The user utilizes one of the secure signature creation devices and one of the smart card readers that were specified in the Security Target.
- Apart from trustworthiness users must check the integrity of the product as described in the user guidance.
- Appropriate virus scanners for the detection of malware, trojan horses or other compromising software are required. If the computer is connected to

the internet, attacks through the Internet must be averted by appropriate means like e.g. the utilization of a firewall.

- The environment of the computer where the TOE is installed on ensures that a user has full control over the computer and shared network storage. It is not possible to gain unauthorised access to the computer via existing network connections.

## 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

The Target of Evaluation (TOE) is called:

### **OPENLiMiT SignCubes base components 2.1, Version 2.1.6.1**

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Date	Form of Delivery
1.	SW	OPENLiMiT SignCubes base components 2.1, version 2.1.6.1	2.1.6.1	23.02.2007	File
2.	SW	Integrity Tool IntegrityTool.jar	see Table 7	07.03.2007	File
3.	DOC	OPENLiMiT SignCubes base components 2.1 – User Guidance (English)	2.1.6.1	21.02.2007	chm-File
4.	DOC	OPENLiMiT SignCubes base components 2.1 – User Guidance (German)	2.1.6.1	21.02.2007	chm-File
5.	DOC	OPENLiMiT SignCubes SDK v2.0 Documentation	1.1	17.05.2006	PDF-File
6.	SW (Header file)	siqSDK.h	see Table 7	10.04.2006	File

No	Type	Identifier	Release	Date	Form of Delivery
7.	SW (Library file)	siqSDK.lib	see Table 7	10.04.2006	File

Table 6: Deliverables of the TOE

The TOE deliverables No.1 to No.4 are delivered to customers who purchase the TOE as a standalone application.

The TOE deliverables No.5 - 7 are intended for developers who want to integrate the API provided by the TOE into their own application.

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

No.	File	SHA-1-value
1.	siqSDK.h	488c09f809df9b6fbbbbb225649dcc890f6b52461
2.	siqSDK.lib	0d7029d0afd70838bcbb9e6e5093f46f19db2d38
3.	IntegrityTool.jar	fa3a26320321e118b0624e42567f8c8e4d774b09

Table 7: 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 4.2.

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 4.2 and
- especially the OPENLiMiT SignCubes 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 functionalities 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 customer 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 OPENLiMiT SignCubes Integrity Tool. This applet is provided by OPENLiMiT SignCubes AG on the website

**<https://www.openlimit.com/integritytool>**

The OPENLiMiT SignCubes 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. 5 – No. 7 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 signature to ensure the integrity and authenticity of the software.

### 3 Security Policy

The OPENLiMiT SignCubes base components 2.1, Version 2.1.6.1 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 unambiguously 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

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

## 4.2 Environmental assumptions

- **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 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

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<sup>13</sup>.

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:

- OPENLiMiT card from Deutsche Telekom AG<sup>14</sup>
- TeleSec E4 NetKey Card from Deutsche Telekom AG
- TeleSec PKS Card v2.0 and v3.0 from Deutsche Telekom AG
- Signtrust signature card SEA-Card v1.0 from Deutsche Telekom AG
- Signtrust signature card SEA-Card v2.0 from Deutsche Telekom AG
- Signature card D-TRUST card version 1.0 from ORGA Kartensysteme GmbH

---

<sup>13</sup> The manual installation of the Microsoft SmartCard base components is required for Microsoft Windows NT 4.0.

<sup>14</sup> Technically identical to the TeleSec E4 NetKey Card from Deutsche Telekom AG

- Signature card D-TRUST card version 1.1 from ORGA Kartensysteme GmbH
- Signature card D-TRUST Card\_MS version 1.0 from ORGA Kartensysteme GmbH
- Signature card DATEV e:secure-card v1.0 from Deutsche Telekom AG
- Signature card DATEV e:secure-card v1.10 from Deutsche Telekom AG
- Signature card DATEV e:secure-card v1.20 from Deutsche Telekom AG
- STARCOS SPK 2.3 v7.0 with digital signature application StarCert v2.2 from Giesecke & Devrient
- STARCOS SPK2.3 with Digital Signature Application StarCert (limited signature generation configuration) from Giesecke & Devrient
- STARCOS SPK2.3 with Digital Signature Application StarCert (unlimited signature generation configuration) from Giesecke & Devrient
- STARCOS 3.0 with Electronic Signature Application V3.0 from Giesecke & Devrient
- Siemens CardOS M4.3 B from Siemens AG
- CardOS V4.3B Re\_Cert with Application for Digital Signature from Siemens AG
- 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
- ZKA Banking signature card, v6.2 NP, Type 3 from Giesecke & Devrient
- ZKA Banking signature card v6.32, Type 3 from Giesecke & Devrient
- ZKA signature card, version 5.10 from Gemplus-mids GmbH<sup>15, 16</sup>
- ZKA signature card, version 5.11 from Gemplus-mids GmbH
- 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 SECCOS Sig v1.5.3 from Sagem Orga GmbH
- S-TRUST signature card release 3 (SPK 2.3 based)

---

<sup>15</sup> The approval has not yet been published by the Bundesnetzagentur.

<sup>16</sup> This smart card is named "ZKA signature card ZKA 680 V5A" in the Security Target

The S-TRUST signature card release 3 is only supported for the purpose of advanced signatures. The qualified signature is not supported for that smart card.

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 Model ST-2000
- Cherry G83-6700 LQ
- Cherry G83-6744 LU
- Kobil B1 Pro USB
- Kobil KAAAN SecOVID Plus
- Kobil Standard Plus
- Kobil KAAAN Advanced
- SCM Microsystems SPRx32
- Reiner SCT cyberJack e-com v2.0
- Reiner SCT cyberJack pinpad v2.0
- Reiner SCT cyberJack pinpad v3.0
- Omnikey Cardman 3621
- Omnikey Cardman 3821
- Omnikey Cardman 8630
- Fujitsu Siemens S26381-K329-V2xx HOS:01

The used components are approved components according to the German signature law with exception of the Omnikey Cardman 8630. The certificates can be obtained from the Bundesnetzagentur ([www.bundesnetzagentur.de](http://www.bundesnetzagentur.de)) if not indicated otherwise.

- **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.

#### **Restrictions and Exceptions**

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

Table 8 depicts which smart card terminals are not supported by the corresponding operating system.

<b>Operating system</b>	<b>Smart card terminal</b>
Windows NT 4 SP 6	Cherry G83-6744 LU
	Cherry ST2000
	Reiner SCT cyberJack pinpad v3.0
	Kobil KAAN Advanced
	Kobil B1 Pro USB
	Fujitsu Siemens S26381-K329-V2xx HOS: 01
	Omnikey Cardman 3621
	Omnikey Cardman 3821
Windows XP 64 Bit Edition	Cherry G83-6700 LQ
	Cherry ST2000
	Kobil KAANAdvanced
	Kobil B1 Pro USB
	Kobil KAAN SecOVID Plus
	Kobil Standard Plus
	SCM SPRx32 (Firmware version 4.15)
Windows 2003	Cherry G83-6700 LQ
Windows Vista	Cherry G83-6700 LQ
	Reiner cyberJack e-com v2.0
	Reiner cyberJack pinpad v2.0
	Kobil KAAN Advanced
	Kobil B1 Pro USB
	Kobil KAAN SecOVID Plus
	Kobil Standard Plus
	Omnikey Cardman 8630
SCM SPRx32 (Firmware version 4.15)	

Table 8: Incompatibility between operating system and smart card terminals

Table 9 depicts the combinations of operating system and smart cards that are incompatible with the smart card terminal Cherry G83-6700 LQ.

<b>Cherry G83-6700 LQ</b>	
<b>Operating system<sup>17</sup></b>	<b>Smart card</b>
Windows NT 4.0 SP 6.0	ZKA Banking Signature card, v6.2 NP Type 3
Windows 2000	ZKA Banking Signature card, v6.2b NP, 6.2f NP, Type 3
Windows 2003	ZKA Banking signature card, v6.31 NP, Type 3
Windows XP	ZKA Banking Signature Card, v6.32, Type 3
	ZKA Banking signature card, Version 6.4
	ZKA Banking signature card, Version 6.51
	ZKA Banking Signature Card, v6.6
	ZKA signature card, version 5.11
	ZKA signature card, version 5.02
	ZKA SECCOS Sig v1.5.3
	STARCOS 3.0 with Electronic Signature Application V3.0

Table 9: Incompatibilities of the smart card terminal Cherry G83-6700 LQ

Table 10 shows the combination between operating systems and smart cards that are not supported by the smart card terminals Kobil KAAN SecOVID Plus and Kobil Standard Plus.

<b>Kobil KAAN SecOVID Plus and Kobil Standard Plus</b>	
<b>Operating system</b>	<b>Smart card</b>
Windows NT 4.0 SP 6.0	Siemens CardOS V4.3B
Windows 2000	CardOS V4.3B Re_Cert with Application for Digital Signature
Windows XP	STARCOS 3.0 with Electronic Signature Application V3.0
Windows XP	ZKA Banking Signature Card, v6.6

Table 10: Incompatibilities of the smart card terminals Kobil KAAN SecOVID Plus and Kobil Standard Plus

<sup>17</sup> If the operating system „Windows XP“ is mentioned, the different versions Windows XP Home, Windows XP Professional, Windows XP Tablet PC Edition and Windows XP 64 Bit Edition are meant.

Table 11 summarizes the combination of operating system and smart cards that cannot be used together with the smart card terminals Cardman 3621, Cardman 3821 and Cardman 8630.

<b>Cardman 3621, Cardman 3821, Cardman 8630</b>	
<b>Operating system</b>	<b>Smart Card</b>
Windows NT 4, SP 6	Signature card D-TRUST card version 1.0
Windows 2000, ab SP 2	Signature card D-TRUST card version 1.1
Windows 2003	
Windows XP	
Windows Vista	
Windows Vista	CardOS V4.3B Re_Cert with Application for Digital Signature

Table 11: Incompatibilities of the smart card terminals Cardman 3621, Cardman 3821 and Cardman 8630

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

## 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 the OPENLiMiT SignCubes base components 2.1 may be used as a single application but also may be integrated into third party products. The TOE comprises three different parts:

- the OPENLiMiT SignCubes Security Environment Manager
- the OPENLiMiT SignCubes Viewer
- the OPENLiMiT SignCubes Integrity Tool

The first two parts represent the main components of the TOE whereas the OPENLiMiT SignCubes Integrity Tool is a separate application implemented as a Java Applet. The OPENLiMiT SignCubes 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.

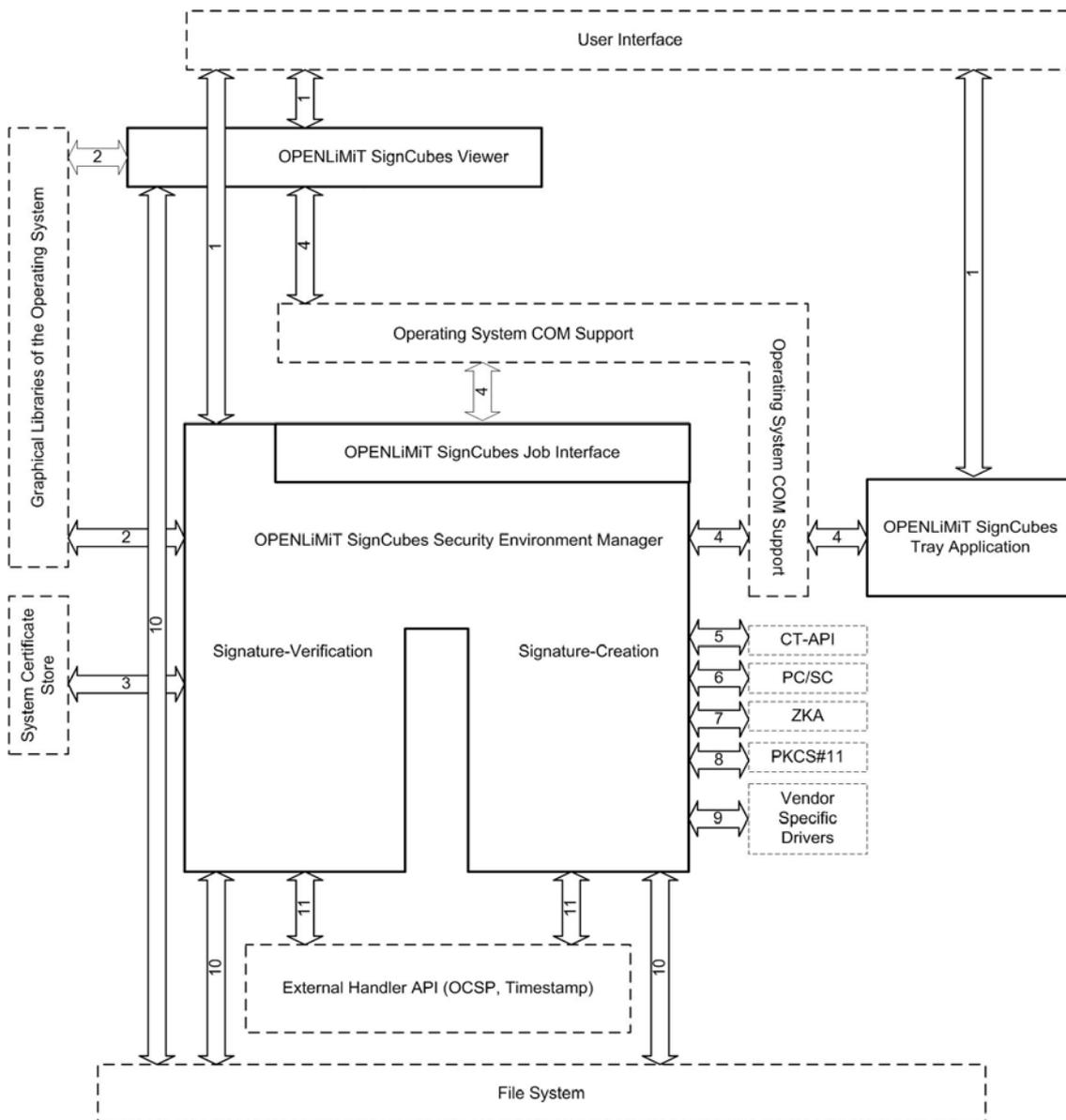


Figure 1: Decomposition of the main components of the TOE

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 4.1 and chapter 4.2 in this report).

The OPENLiMiT SignCubes Viewer is a software component for displaying signed data or data to be signed according to the signature law §17 paragraph 2. The OPENLiMiT SignCubes 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 OPENLiMiT SignCubes Viewer, he can start the process of electronic signature creation using the OPENLiMiT SignCubes Viewer as an indirect interface to that

functionality provided by the OPENLiMiT SignCubes Security Environment Manager.

The OPENLiMiT SignCubes Security Environment Manager provides the following functionality that may be accessed in parts or completely through the use of the OPENLiMiT SignCubes 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 OPENLiMiT SignCubes base components installed on the user's computer.
- Providing graphical interfaces in the process of signature creation, verification and product configuration

## 6 Documentation

The product OPENLiMiT SignCubes base components 2.1 is provided with the following documentation:

The user guidance [9] and [10] contains important instruction about the operation of the TOE, installation, errors and usage. The guidance of the OPENLiMiT SignCubes SDK [11] provides the information that developers of third party products need to use the provided API correctly in a secure manner.

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.

The developer provides further instructions for the download and secure installation of the add-on setups. The user must act in accordance with these instructions.

## **7 IT Product Testing**

### **7.1 Developer tests**

The tests of the developer were conducted with the smart cards, smart card terminals and operating systems listed in chapter 4.2, assumption A.Platform and thus in accordance with the ST [6]. All additional prerequisites mentioned in the assumptions on the operating environment (see chapter 1.6 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 fulfilled 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.

### **7.2 Evaluator tests**

Due to the evaluation assurance level EAL4+ 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 eliminated.

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

### **7.3 Test results**

The tests showed that the TOE behaves as expected. The depth of testing is adequate for the evaluation assurance level chosen (EAL4+). 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 OPENLiMiT SignCubes base components 2.1 Version 2.1.6.1 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

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 coordination with the Certification Body [4, AIS 34]).

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

The verdicts for the CC, Part 3 assurance components (according to EAL4 augmented by AVA\_VLA.4 and AVA\_MSU.3) 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

Assurance classes and components		Verdict
Problem tracking 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
Fully defined external interfaces	ADV_FSP.2	PASS
Security enforcing high-level design	ADV_HLD.2	PASS
Subset of the implementation of the TSF	ADV_IMP.1	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Informal TOE security policy model	ADV_SPM.1	PASS
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
Identification of security measures	ALC_DVS.1	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Well-defined development tools	ALC_TAT.1	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: high-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 12: Verdicts for the assurance components

The changes that were evaluated during this re-certification comprise the addition of smart cards and smart card terminals, improvements in the support of smart cards implementing other hash algorithms than SHA-1 (e.g. SHA-256 or RIPEMD-160) and changes of the source code to improve the general coding quality.

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). This holds for

- (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 results of the evaluation are only applicable to the OPENLiMiT SignCubes base components 2.1, Version 2.1.6.1 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 provided 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 digital signatures the TOE uses the RSA-Algorithms with bitlengths between 1024-2048 bits. According to the publication of the Bundesnetzagentur, 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.

The following table describes the validity period of hash functions according to the publication of the Bundesnetzagentur [15].

Hash function	Valid until end of
SHA-1	2009
RIPEND 160	2010
SHA-256, SHA-384, SHA-512	2012

Table 13: Validity period of hash functions

As the OPENLiMiT SignCubes base components 2.1 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	2012

Table 14: 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](http://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

<b>API</b>	Application Programming Interface
<b>BSI</b>	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
<b>CC</b>	Common Criteria for IT Security Evaluation
<b>CRL</b>	Certificate Revocation List
<b>CT</b>	Card Terminal
<b>EAL</b>	Evaluation Assurance Level
<b>IT</b>	Information Technology
<b>OCSP</b>	Online Certificate Status Protocol
<b>PC/SC</b>	Personal Computer/Smart Card
<b>PP</b>	Protection Profile
<b>SDK</b>	Software development kit
<b>SF</b>	Security Function
<b>SFP</b>	Security Function Policy
<b>SOF</b>	Strength of Function
<b>SSCD</b>	Secure Signature Creation Device
<b>ST</b>	Security Target
<b>TOE</b>	Target of Evaluation
<b>TSC</b>	TSF Scope of Control
<b>TSF</b>	TOE Security Functions
<b>TSP</b>	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.

**TSP 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 2.3, 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.
- [5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site
- [6] Security Target BSI-DSZ-0432-2007, Version 1.8, 04/10/2007, Security Target (ST) Electronic Signature Application OPENLiMiT SignCubes base components 2.1 Version 2.1.6.1, OpenLiMiT SignCubes AG
- [7] Evaluation Technical Report, Version 1.2, 04/24/2007, "Evaluation Technical Report BSI-DSZ-CC-0432 BSI.02091.TE.xx.200x" (confidential document)
- [8] Configuration List for OPENLiMiT SignCubes base components 2.1, v2.1.6.1, 04/24/2007, OPENLiMiT SignCubes AG

### Guidance documentation

- [9] User Guidance, Version 2.1.6.1, 02/21/2007, OPENLiMiT SignCubes base components 2.1 – User Guidance (German), OPENLiMiT SignCubes AG
- [9] User Guidance, Version 2.1.6.1, 02/21/2007, OPENLiMiT SignCubes base components 2.1 – User Guidance (English), OPENLiMiT SignCubes AG
- [10] API Documentation, Version 1.1, 05/17/2006, OPENLiMiT SignCubes SDK v2.0 Documentation, OPENLiMiT SignCubes AG

### Legal regulations

- [11] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG)<sup>1)</sup> 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 April 12, 2007, in the Bundesanzeiger No. 69, p. 3759 and available on the web-pages of the Bundesnetzagentur ([www.bundesnetzagentur.de](http://www.bundesnetzagentur.de)).

## 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:

- a) **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.
- b) **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:

- a) **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.
- b) **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:

- a) **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.
- b) **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:

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

CC Part 3:

**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.“



# Certification Report

**Bundesamt für Sicherheit in der Informationstechnik**

**BSI-DSZ-CC-0432-2007**

for

**OPENLiMiT SignCubes base components 2.1  
Version 2.1.6.1**

from

**OPENLiMiT SignCubes AG**

**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."

**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."