Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0397-2008

for

Sign Live! CC
Version 3.2.3

from

intarsys consulting GmbH

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0397-2008

Signaturanwendungskomponente

Sign Live! CC
Version 3.2.3

from	intarsys consulting GmbH
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL3 augmented by ADO_DEL.2 - Detection of modification ADV_IMP.1 - Subset of the implementation of the TSF ADV_LLD.1 - Descriptive low-level design ALC_TAT.1 - Well-defined development tools AVA_MSU.3 - Analysis and testing for insecure states AVA_VLA.4 - Highly resistant

Common Criteria
Recognition
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 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, 29 August 2008
For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

Bernd Kowalski
Head of Department

L.S.

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] 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

2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Mutual Recognition Agreement (MRA) for 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 Assurance 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.

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

As of 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 Recognition 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 Sign Live! CC 3.2.3 Version 3.2.3 has undergone the certification procedure at BSI.

The evaluation of the product Sign Live! CC 3.2.3 was conducted by T-Systems GEI GmbH. The evaluation was completed on 16 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 developer, sponsor and applicant is: intarsys consulting GmbH.

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

[6] Information Technology Security Evaluation Facility

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.

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 Sign Live! CC 3.2.3 has been included in the BSI list of the certified products, which is published regularly (see also Internet: https:// www.bsi.bund.de) and [5]. Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] intarsys consulting GmbH
Bahnhofplatz 8
76137 Karlsruhe

B Certification Results

The following results represent a summary of

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

1 Executive Summary

The Target of Evaluation (TOE) is a signature creation application (SCA, according to [13]), which offers the following functions:

- Creation of an advanced or qualified electronic signature for a single or a set of documents. For qualified signature creation a SSCD is needed.
- Validation of electronic signatures for a single or a set of documents.
- Legal binding displaying of documents in PDF, TEXT and TIFF format and functions to examine the content of the document(s) to be signed/validated.

Sign Live! CC connects SSCDs for usage in a standard workplace environment with card terminal (CT) via Sign Live! CC's trusted smart card adapters.

Sign Live! CC also provides a command line interface, which offers the user the option to call the mentioned functions via operating system calls.

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

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the Assurance Requirements of the Evaluation Assurance Level EAL 3 augmented by ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3, 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. OPENEDDOCUMENT FALSIFICATIONPREVENTION	If the user starts the signing process the TOE calculates the hash value of the document that was previously loaded into the memory. After the signature returns from the SSCD the TOE compares the signed hash value with the calculated hash value to prevent a falsification of the document during the signing process.
SF. SELECTEDDOCUMENT FALSIFICATIONPREVENTION	If the user selects a document for batch processing the TOE calculates a fingerprint of the document in the moment of selection. When the batch process starts the TOE recalculates the fingerprint and compares the two values. If they differ the user is informed that the document was changed between the selection and the start of the batch process.
SF.SIGNATURECREATION	The TOE allows to sign documents either interactively by the user or during a batch processing. For an interactive signature creation of one selected document the TOE informs the user unambiguously that an electronic signing process begins and - if desired by the user - presents the document in a Trusted Viewer. The TOE transmits the original hash value to a connected SSCD and returns the completed

TOE Security Function	Addressed issue
	signature in a corresponding digital data structure. The electronic signature itself is calculated outside the TOE on the SSCD. For batch processing the user selects a set of documents and starts the signing process after being unambiguously informed by the TOE. The TOE calculates the number of documents to be signed and requests exactly this number of signatures from a connected SSCD. The TOE initiates an exclusive connection to the SSCD, requests the SSCD pin only once and closes this connection after receiving the last signature or when user stops the process. The pin must be entered on the card terminal that holds the smart card. Apart from the starting the batch process via the GUI of the TOE the command line interface allows to use the corresponding functions with appropriate system calls.
SF.SIGNATUREVALIDATION	The TOE verifies electronically signed documents, i.e. it validates the document's signature, constructs a corresponding certificate chain and validates the certificate chain's signature(s). Additionally all certificates are checked for revocation information. The validation algorithm handles OCSP responses and timestamps which are eventually contained in the signature. The user can select a single document or a set of documents for batch processing. In case of batch processing the results are not only presented in the GUI but also stored on the hard disk. If the validation batch process is started via the command line interface the results are only stored in the file system.
SF.OCSPPROCESSING	To validate a certificate the TOE is able to interpret the information contained in an OCSP response. The OCSP response is either contained in the digital data structure representing the signature to be validated or is delivered by an OCSP handler.
SF.TIMESTAMPVALIDATION	The TOE is able to verify timestamps given in a signature. For this the timestamp creator's certificate must be known to the TOE either by a certificate store the TOE has access to or because it was delivered together with the timestamp. Otherwise the timestamp will not be validated.
SF.DOCUMENTPRESENTATION	The TOE ensures the unambiguous presentation of a Text-, PDF- or TIFF-document to the user. The TOE reports offences against the built-in rules for each format (e.g. hidden text, active content).
SF.TOEINTEGRITYCHECKING	TOE assures its integrity by the following mechanisms: – A user may view component information which indicates the TOE's name, release, certification and confirmation ID. – The active Trusted Mode indicates that the TOE is correctly configured to create and validate qualified signatures. The TOE indicates the Trusted Mode by an icon in the status bar and in the application log. – The installed TOE components are digitally signed with a Code Signing Private Key issued by a trusted CA (Thawte). The Sign Live! CC Installation Verifier is a TOE component that verifies the digital signatures by means of the Code Signing Certificate and the hash values of valid products. It is available on the intarsys homepage www.intarsys.de. The Sign Live! CC Installation Verifier is realized as a Java Applet

TOE Security Function	Addressed issue
	and also signed with the above mentioned intarsys Code Signing Certificate so that standard browsers can verify the authenticity and consistency of the applet.

Table 1: TOE Security Functions

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

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 3.2. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

This certification covers the configuration of the TOE in the Trusted Mode. For details refer to chapter 8.

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:

Sign Live! CC 3.2.3

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Date	Form of Delivery
1	SW	Sign Live! CC 3.2.3	3.2.3	03.04.2008	File
2	SW	Sign Live! CC Installation Verifier	3.2.3	03.04.2008	File
3	DOC	README		30.01.2008	Contained in the deployed product as PDF document.
4	DOC	Sign Live! CC - User Guidance	3.2.3	14.04.2008	Contained in the deployed product as Java Help.

Table 2: Deliverables of the TOE

The TOE is available on CD or from the homepage of intarsys consulting GmbH. All guidance documents and the Sign Live! CC 3.2.3 software are contained in two different installation assistants that either contain the JRE required to run the application or not. The Sign Live! CC Installation Verifier can be downloaded from the homepage of the developer only. The download page is secured with a SSL-certificate issued for the intarsys consulting GmbH.

After a user completes the installation the Sign Live! CC Installation Verifier must be executed to check the integrity of the product installation.

3 Security Policy

The TOE is a signature creation application that claims conformance to the German Signature Law §17, par. 2 and German Ordinance on Electronic Signatures §15, par.2 and 4. Thus it enforces the following Security Policy that is expressed by the set of Security Functional Requirements and implemented by the TOE.

- 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 enforces the rule that a signature is provided only at the initiation of the authorized signing person.
- The TOE shows to which data the signature refers, whether the signed data are unchanged and to which signature-code owner the signature is to be assigned.
- For the verification of a qualified electronic signature the TOE reliably verifies the correctness of a signature and displays this fact appropriately.
- The TOE presents the contents of the qualified certificate on which the signature is based and the results of the subsequent check of certificates.
- 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.
- If data to be signed or data already signed is displayed by the TOE certain rules for the treatment of nonreadable signs are enforced.
- 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:

- In the environment at least one of the supported smart card terminals must be connected to the workstation that runs the TOE.
- The used hard- and software components have to meet the requirements defined in Security Target, chapter 2.6.1.
- The system on which the TOE is installed may have internet access. In this case a firewall and a virus scanner must be used to prevent compromising by internet attacks and to detect malicious programs installed on the system.
- The user has full control about inserted storage devices of the system, on which the TOE is installed. The TOE is protected in such a way that it is not possible to access parts of the TOE or its working directories through existing network connections.
- Users and administrators are trustworthy and follow all user guidance. Especially the user verifies the TOE’s integrity as described in the user guide.
- In the case the TOE is operated without GUI, the user should take sufficient precautions to protect the TOE’s working directories against unauthorised

manipulation, to be sure that the documents selected for the signature process won't be manipulated in the time between optional viewing the documents and starting the signature process.

Details can be found in the Security Target [6] chapter 3.

5 Architectural Information

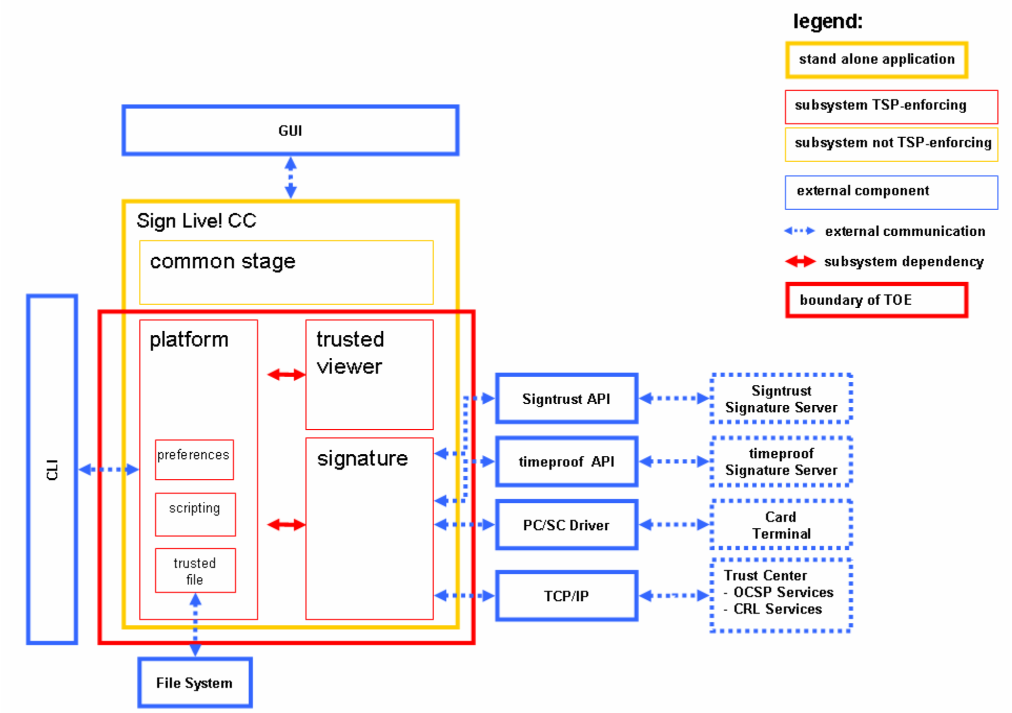

Figure 1: Architecture of the TOE on the client PC

Figure 1 depicts the subsystems of the TOE that are installed on the client computer. The blue-bordered boxes represent the interfaces of the TOE to the environment. The red-framed box is the part of the TOE that enforces the TOE security policy and contains the following subsystems:

- platform: The subsystem provides a framework providing the application's extension as well as basic functionality such as:
  - Load, view, save and print a document,
  - control the application using the command line,
  - configure the application,
  - secure file system access,
  - script processing, batch processing,
  - verify the application's integrity and configuration state
- signature: The functionality offered by this subsystem basically comprises:
  - Sign a document,
  - verify and inspect a document's integrity,
  - create a validation report for a document,

  - verify and inspect a certificate,
  - sign a set of documents (batch signing),
  - validate a set of documents (batch validation),
  - calculate a digest for any byte array

- trusted viewer: The subsystem covers the security requirements considering secure display of a document. The provided functionality basically covers:
  - Get a straight view on a document as it is specified
  - Inspect a document's internal structure

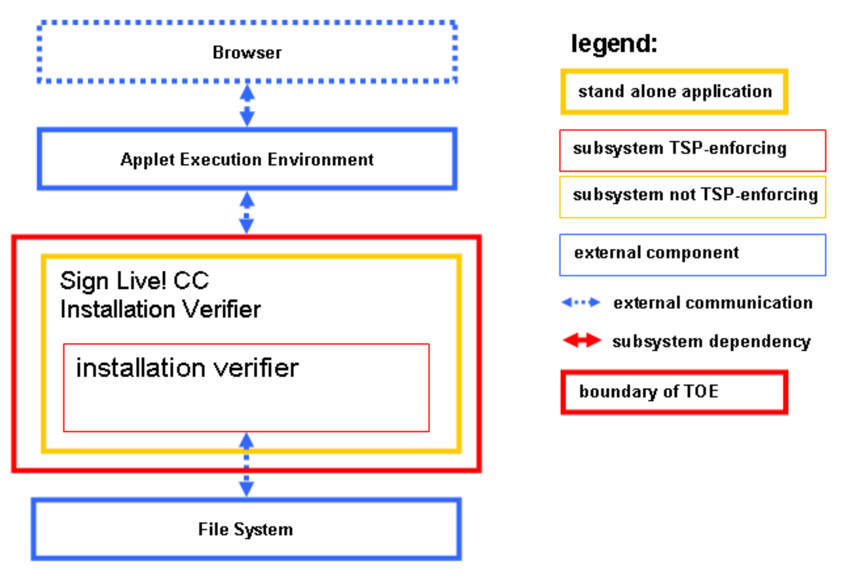

Figure 2: Architecture of the Sign Live! CC Installation Verifier

As described above the user must check the integrity of the installation by means of the Sign Live! CC Installation Verifier. Figure 2 shows the architecture of this part of the TOE.

The Sign Live! CC Installation Verifier contains only the subsystem “Installation verifier”. The subsystem offers the possibility to verify the application's integrity. The verification procedure answers the following questions:

- Has the application been modified since its creation?
- Which modifications were applied to the application?
- Has the installed application version been officially released by the application vendor?

6 Documentation

The evaluated documentation as outlined in table 2 is provided together 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

The developer tested each TSF defined in the Security Target [6] for the TOE. These tests cover all configurations regarding the combinations of operating system, smart cards and smart card readers that are listed in the Security Target. The tests only cover the configuration of the TOE in the Trusted Mode.

The test description demonstrates that the developer performed his testing on a subsystems level and the testing effort meets the requirements of the chosen components of the SAR-class ATE. The test effort of the developer demonstrates that the security functionality defined in the security target is implemented as required.

The evaluators adequately tested the claimed resistance of the TOE against attackers with high attack potential. The evaluators spent several days each

- for analysing the test specification,
- for creating ideas of independent evaluator tests,
- for ensuring that the test environment delivers correct test results and
- for repeating developer tests as well as carrying out independent tests.

According to EAL3, independent testing is performed down to a depth of subsystem interfaces. The tests showed that the TOE behaves as expected. The depth of testing is adequate for the evaluation assurance level chosen (EAL3+). The TOE has successfully passed independent testing.

The evaluators decided to test several potential vulnerabilities to ensure that these potential vulnerabilities do not exist in the TOE. The penetration tests performed by the evaluators confirmed that the potential vulnerabilities found by the evaluators are not existent within the TOE.

The evaluators used the following testbed for independent and penetration testing:

- operating systems:
  - Windows XP Home,
  - Windows XP Professional,
  - Windows XP Tablet PC Edition,
- smart cards:
  - Giesecke & Devrient: STARCOS 3.0 with Electronic Signature Application V3.0 with Initializing Tables Signtrust Card 3.0 und Signtrust MCard 3.0 (single + batch)
  - Gemplus ZKA-Signaturkarte, Version 5.11 (single)
  - Gemplus ZKA-Signaturkarte, Version 5.11 M (batch)
- smart card terminals:
  - KOBIL KAAN Advanced Firmware Version 1.02, Hardware Version K104R3
  - KOBIL SecOVID Reader III
  - OMNIKEY CardMan Trust CM3821, Firmware-Version 6.00
  - Reiner SCT cyberJack e-com, Version 2.0

8 Evaluated Configuration

The certificate covers the TOE in the Trusted Mode. The Trusted Mode is active if:

- configuration for validation is either SigG or EU
- Java Script Live Connect Feature (Java API available in JavaScript) is deactivated for document scripting

TOE indicates the Trusted Mode by an icon in the status bar and in the application log. The user guidance describes how the user is able to set the Trusted Mode. User settings or manipulation of the TOE may result in a configuration that differs from the Trusted Mode, but in this case the corresponding icon is not shown in the status bar.

Furthermore the certificate extends only to the TOE that is listed in Table 2 and was installed by means of one of the delivered installation assistants.

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 up to EAL4 extended by advice of the Certification Body for components beyond EAL 4 [4] (AIS 34).

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 EAL3 package as defined in the CC (see also part C of this report)
- The components ADO_DEL.2, ADV_IMP.1, ADV_LLD.1, ALC_TAT.1, AVA_MSU.3, AVA_VLA.4 augmented for this TOE evaluation.

The evaluation has confirmed:

- for the Functionality: Product specific Security Target Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL3 augmented by
  ADO_DEL.2 - Detection of modification
  ADV_IMP.1 - Subset of the implementation of the TSF
  ADV_LLD.1 - Descriptive low-level design
  ALC_TAT.1 - Well-defined development tools
  AVA_MSU.3 - Analysis and testing for insecure states
  AVA_VLA.4 - Highly resistant

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

- hash functions:

  SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, RIPEMD-160

- algorithms for the decryption in the context of digital signature verification:

  RSA with bit length of 1024 up to 2048 bits.

This holds for the following security functions:

- SF.OPENEDDOCUMENTFALSIFICATIONPREVENTION,
- SF.SELECTEDDOCUMENTFALSIFICATIONPREVENTION,
- SF.SIGNATURECREATION,
- SF.SIGNATUREVALIDATION,
- SF.OCSPPROCESSING,
- SF.TIMESTAMPVALIDATION and
- SF.TOEINTEGRITYCHECKING

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 [13] the algorithms are suitable for the creation and validation of qualified electronic signatures. The validity period of each algorithm is mentioned in the official catalogue [13] and summarized in chapter 10.

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

- The user should assure that the TOE runs in a certified configuration before a digital signature is created or verified. This includes especially a regular inspection of the installation integrity by means of the Sign Life! CC Installation Verfifier.
- The strength of a digital signatures heavily depends on the algorithms used for hashing of documents and encryption of the hash value. Therefore each algorithm employed in the context of qualified electronic signature has a validity period that is published in the official catalog [15]. The limit of each validity period relevant for this product is summarised in the following tables.

Hash function	**Valid until end of**
SHA-1,	Validity expired for the creation of qualified electronic signatures
RIPEMD-160	2010
SHA-224, SHA-256, SHA-384, SHA-512,	2014

Table 3: Validity period of hash functions

The following table shows the validity period for the different bit lengths of the RSA algorithm.

RSA bit length	Valid until end of
1024	Validity expired for the creation of qualified electronic signatures
1280	2008
1536	2009
1728	2010
1976	2014

Table 4: Validity period for the bit length of the RSA-Algorithm

In general the Bundesnetzagentur recommends to use a bit length of 2048 bit for the RSA-Algorithm to ensure a long-term security of qualified electronic signatures.

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

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CA	Certificate Authority
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
SAR	Security Assurance Requirement
SCA	Signature Creation Application
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
SSCD	Secure Signature Creation Device
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 Methology for Information Technology Security Evaluation (CEM), Evaluation Methology, 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.[8]

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

[6] Security Target BSI-DSZ-0397-2008, Version 1.12, Sign Live! CC 3.2.3 Security Target, 25.04.2008, intarsys consulting GmbH

[7] Evaluation Technical Report, Version 1.0, 25.04.2008, Evaluation Technical Report BSI-DSZ-CC-0397, T-Systems GEI GmbH (confidential document)

[8] Configuration list for the TOE, 25.04.2008, Konfigurationslisten.ZIP (confidential files)

[9] Sign Live! CC - User Guidance, 14.04.2008, Online Help

[10] CEN Workshop Agreement CWA 14170, May 2004, EUROPEAN COMMITTEE FOR STANDARDIZATION

[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), 04.01.2005, BGBl. volume 2005 part I p. 2

[12] Verordnung zur elektronischen Signatur (Signaturverordnung - SigV), 16.11.2001, BGBl. volume 2001 part I p. 876

[8] specifically

- AIS 25, Version 3, 6 August 2007, Anwendung der CC auf Integrierte Schaltungen including JIL Document resp. CC Supporting Document
- AIS 26, Version 3, 6 August 2007, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document resp. CC Supporting Document
- AIS 31, Version 1, 25 Sept. 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document resp. CC Supporting Document and CCRA policies
- AIS 36, Version 2, 12 November 2007, Kompositionsevaluierung including JIL Document resp. CC Supporting Document
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[13] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), published 05.02.2008, Bundesanzeiger No. 19, p. 376 and available for download on the web-pages of the Bundesnetzagentur (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:

- **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.

This page is intentionally left blank.