Federal Office
for Information Security

# Certification Report

**BSI-DSZ-CC-0476-2007**

for

**CardOS V4.2B FIPS**
**with Application for Digital Signature**
**running on Infineon Chips SLE66CX322P and SLE66CX642P**

from

**Siemens AG**

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

# Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

**BSI-DSZ-CC-0476-2007**

Smart Card with Signature Application

**CardOS V4.2B FIPS with Application for Digital Signature running on Infineon Chips SLE66CX322P and SLE66CX642P**

| | |
|---|---|
| from | Siemens AG |
| PP Conformance: | Protection Profile BSI-PP-0006-2002 |
| Functionality: | PP conformant<br>plus product specific extensions<br>Common Criteria Part 2 extended |
| Assurance: | Common Criteria Part 3 conformant<br>EAL 4 augmented by<br>AVA_VLA.4, AVA_MSU.3 |

Common Criteria
Arrangement
for components up
to EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using *the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for* components beyond EAL 4 and guidance specific for the technology of the product for conformance to the *Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)*.

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 29. November 2007

The President of the Federal Office
for Information Security

IT Security Certified

SOGIS - MRA

Dr. Helmbrecht 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)
- 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] 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 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

## 2.1 European Recognition of ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998.

This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognises certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

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

## 2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 has been signed in May 2000 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC.

As of February 2007 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations resp. approved certification schemes can be seen on the web site: http:\\www.commoncriteriaportal.org

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

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

# 3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product CardOS V4.2B FIPS with Application for Digital Signature running on Infineon Chips SLE66CX322P and SLE66CX642P has undergone the certification procedure at BSI.

The evaluation of the product CardOS V4.2B FIPS with Application for Digital Signature running on Infineon Chips SLE66CX322P and SLE66CX642P was conducted by T-Systems GEI GmbH. The evaluation was completed on 08. October 2007. The T-Systems GEI GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant is: Siemens AG.

The product was developed by: Siemens AG.

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

# 4 Validity of the certification result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report and in the Security Target.

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.

---

[6] Information Technology Security Evaluation Facility

# 5 Publication

The following Certification Results contain pages B-1 to B-18 and D1 to D-4.

The product CardOS V4.2B FIPS with Application for Digital Signature running on Infineon Chips SLE66CX322P and SLE66CX642P has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[7] Siemens AG
Medical Solutions
MED GS SEC DS
Charles-de-Gaulle-Str. 2-3
81737 München, Germany

# 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

The TOE CardOS V4.2B FIPS with Application for Digital Signature running on Infineon Chips SLE66CX322P and SLE66CX642P is a Secure Signature-Creation Device (SSCD) according to Directive 1999/93/ec of the European parliament and of the council of 13 December 1999 on a Community framework for electronic signatures [7].

The TOE consists of configured software (OS, packages and signature application), the underlying hardware (SLE66CX322P/ SLE66CX642P from Infineon) used to implement the Secure Signature-Creation Device (SSCD) and the pertaining guidance documentation 'Administrator Guidance CardOS V4.2B_FIPS' [11] and 'User Guidance CardOS V4.2B_FIPS' [12].

CardOS V4.2B is a multifunctional smart card operating system (OS) supporting active and passive data protection.

The Security Target [6] is based on the certified Protection Profile BSI-PP-0006-2002, Version 1.05 [9].

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see part C of [1], part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by AVA_MSU.3 and AVA_VLA.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 5. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC part 2 extended.

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

| **TOE Security Function** | **Addressed issue** |
|---|---|
| SF1 | User Identification and Authentication |
| SF2 | Access Control |
| SF3 | SCD/SVD Pair Generation |
| SF4 | Signature Creation |
| SF5 | Protection |
| SF6 | Secure Messaging |
| SF7 | SVD Transfer |

Table 1: TOE Security Functions

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

The claimed TOE's strength of functions 'high' (SOF-high) for specific functions as indicated in the Security Target [6], chapter 6.3 is confirmed. The rating of the strength of functions does not include the cryptoalgorithms suitable for

encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3. Based on these assets the security environment is defined in terms of assumptions, threats and policies. This is outlined in the Security Target [6], chapter 3.1, 3.2 and 3.3.

This certification covers the following configurations of the TOE

- CardOS V4.2B with FIPS packages and applications based on the Infineon SLE66CX322P Integrated Circuit Card (ICC) platform including HMAC package signature application.
- CardOS V4.2B with FIPS packages and applications based on the Infineon SLE66CX642P ICC platform including HMAC package signature application.
- CardOS V4.2B with FIPS packages and applications based on the Infineon SLE66CX322P ICC platform without HMAC package signature application.
- CardOS V4.2B with FIPS packages and applications based on the Infineon SLE66CX642P ICC platform without HMAC package signature application.

The Post- and Preloaded scenarios, described in Chapter 2 are included. More details about configuration testing are given in 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:

**CardOS V4.2B FIPS with Application for Digital Signature running on Infineon Chips SLE66CX322P and SLE66CX642P**

The following table outlines the TOE deliverables:

| No | Type | Term | Release | Form of Delivery |
|---|---|---|---|---|
| 1 | SW Operating System | CardOS V4.2B | C809 | loaded in ROM / EEPROM |
| 2 | SW Application Digital Signature (Application / Data Structure) | **Pre-loaded variant:** | | Personalization Script Files in Python format, after whose execution the ADS will be loaded in EEPROM |
| | | V42B_FIPS_InitScript.py | 1.1 | |
| | | V42B_FIPS_InitScript_DF_DS_x.py | 1.0 | |
| | | V42B_FIPS_PersScript.py | 1.1 | |
| | | V42B_FIPS_PersScript_DF_DS_x .py | 1.1 | |
| | | V42B_FIPS_CAScript.py | 1.1 | |
| | | V42B_FIPS_CAScript_DF_DS_x.py | 1.0 | |
| | | V42B_FIPS_RAScript.py | 1.1 | |
| | | V42B_FIPS_RAScript_DF_DS_x.py | 1.2 | |
| | | **Post-loaded variant** | | |
| | | V42B_FIPS_InitScript_Post.py | 1.1 | |
| | | V42B_FIPS_LRAScript_Post.py | 1.1 | |
| | | V42B_FIPS_LRAScript_Post_DF_DS_x.py | 1.1 | |
| | | **All variants** | 1.0 | |
| | | V42B_FIPS_Default_1024.py | | |
| | | V42B_FIPS_Default_1280.py | | |
| | | V42B_FIPS_Default_1536.py | | |
| | | V42B_FIPS_Default_1752.py | | |
| | | V42B_FIPS_Default_1880.py | | |
| 3 | SW CommandSet_ Extension Package | V42B_CommandSet_Ext_Package.csf | 1.2 | Personalization Script Files in CSF format, after whose execution the resp. code will be loaded and activated in EEPROM |
| 4 | SW CAT Package | V42B_CAT_Package.csf | 1.2 | |
| 5 | SW DRNG Package | V42B_DRNG_Package.csf | 1.3 | |
| 6 | SW WIPE Package | V42B_WIPE Package.csf | 1.1 | |

| No | Type | | Term | Release | Form of Delivery |
|---|---|---|---|---|---|
| 7 | SW HMAC Package (optional) | | V42B_HMAC_Package.csf | 1.2 | |
| 8 | Documentation | | CardOS V4.2B User's Manual | 1.0 | Paper form or PDF-File |
| 9 | Documentation | | CardOS V4.2B Packages & Release Notes | 1.0 | |
| 10 | Documentation | | CardOS V4.2B CAT_DRNG_WIPE Packages & Release Notes | 1.0 | |
| 11 | Documentation | | Administrator Guidance CardOS V4.2B FIPS | 1.4 | |
| 12 | Documentation | | User Guidance CardOS V4.2B FIPS | 1.4 | |
| 13 | Documentation | | ADS_Description CardOS V4.2B FIPS | 1.0 | |
| 14 | Hard-ware (Chip) | 32K | Infineon SLE66CX322P | m1484b14 and m1484f18 | Module |
| | | 64K | Infineon SLE66CX642P | m1485b16 | |
| | Firmware RMS | | RMS | 1.5 | loaded in reserved area of User ROM |
| | Software crypto library | | RSA2048 crypto library | 1.30 | loaded in ROM |
| 17 | Software STS | | STS Self Test Software | V53.10.13 | Stored in Test ROM on the IC |

Table 2: Deliverables of the TOE

Additionally the developer delivers a complete set of Phyton libraries and scripts to aid the personalization process, which are listed in table 3. These libraries and scripts are not part of the TOE.

| Term | Release | Form of Delivery |
|---|---|---|
| cardlib.py | 1.0 | Cardlib Script Files in Python format which are not part of the TOE (necessary for execution of the Personalization Scripts) |
| Apdu.py | 1.14 | |
| Chips.py | 1.2 | |
| codeLen.py | 1.6 | |
| Constants.py | 1.33 | |
| CsfParser.py | 1.9 | |
| DevInifile.py | 1.10 | |
| DirectInterface.py | 1.16 | |
| EchoAPDU.py | 1.9 | |
| EchoInterface.py | 1.7 | |
| Exceptions.py | 1.4 | |
| __init__.py | 1.0 | |
| ExpandedRules.py | 1.2 | |

| Term | Release | Form of Delivery |
|---|---|---|
| Interface.py | 1.13 | |
| InterfaceToCard.py | 1.16 | |
| Iso.py | 1.26 | |
| locate.py | 1.39 | |
| m_classes.py | 1.29 | |
| m_functions.py | 1.17 | |
| m3constants.py | 1.1 | |
| m4lib.py | 1.0 | |
| MAC.py | 1.0 | |
| MAC3.py | 1.0 | |
| makeOptions.py | 1.2 | |
| OsVersionCNS.py | 1.5 | |
| OsVersionHPC1.py | 1.15 | |
| OsVersionM3.py | 1.3 | |
| OsVersionM4.py | 1.33 | |
| OsVersionM401.py | 1.2 | |
| OsVersionM401a.py | 1.2 | |
| OsVersionM401x.py | 1.2 | |
| OsVersionM401y.py | 1.3 | |
| OsVersionM403.py | 1.25 | |
| OsVersionM410.py | 1.15 | |
| OsVersionM420.py | 1.4 | |
| OsVersions.py | 1.11 | |
| OsVersionV42B.py | 1.7 | |
| OsVersionV42BCNS.py | 1.2 | |
| OsVersionV42CNS.py | 1.2 | |
| OsVersionV43.py | 1.4 | |
| OsVersionV43B.py | 1.4 | |
| OsVersionV43BCNS.py | 1.3 | |
| OsVersionV43CNS.py | 1.2 | |
| Pcsc.py | 1.13 | |
| setBaudRate.py | 1.1 | |
| SM.py | 1.24 | |
| tracer.py | 1.4 | |
| translateAddr.py | 1.2 | |
| xd.py | 1.3 | |
| romkeys.py (Default keys) | 1.26.1.0 | |
| reader.ini | 1.0 | Card Reader configuration file (not part of the TOE) |

| Term | Release | Form of Delivery |
|---|---|---|
| M3_Crypto.dll | 1.2 | Crypto Library components (used for SM calculation and not part of the TOE) |
| Des_crypt.dll | 1.2 | |
| rsa_crypt.dll | 1.1 | |
| m3lib.pyd | 1.5 | |
| Python-2.3.4.exe | 2.3.4 | Python Programming Language (not part of the TOE) |
| Python Cryptography Toolkit | 2.0.1 | Python CryptoLibrary (used for SM calculation and not part of the TOE) |

Table 3: additional libraries and scripts which are out of the scope

The chip SLE66CX322P is certified for two production sites: Dresden in Germany (production line indicator '2') and Corbeil Essonnes (called Altis) in France (production line indicator '5')) (see [17], [19] – [21].). The chip SLE66CX642P is certified for the production site Dresden [18].

Two different delivery scenarios are possible:

Scenario 1: Pre-loaded Digital Signature Application: The digital signature application data are put on the card before issuing it to the user. In order to request a certificate, the future Card Holder must be present at the LRA.

Scenario 2: Post-loaded Digital Signature Application: The card is issued without the data for the digital signature application, but with specific information (keys) necessary to load the digital signature data in a secure way at a later time. In this scenario, the card issuer can sell the digital signature application(s) as a separate service.

The TOE is provided to the end-user in form of a smart card as SSCD.

# 3 Security Policy

The security policy is expressed by the set of security functional requirements and implemented by the TOE. It covers the following issues:

The TOE implements the Signature Creation Data (private key) used for signature creation under sole control of the signatory. The TOE implements all IT security functionality which is necessary to ensure the secrecy of the SCD. To prevent the unauthorised usage of the SCD the TOE provides user authentication and access control.

As the TOE is a hardware security platform, the security policy of the TOE is also to provide protection against physical attacks through the TOE interfaces, against storing, copying, and releasing of the signature-creation data, against deriving the signature-creation data, against forgery and against misuse of the signature-creation function of the TOE. Hence the TOE shall

- maintain the integrity and the confidentiality of data stored in the memory of the TOE and
- maintain the integrity, the correct operation and the confidentiality of Security Functions (security mechanisms and associated functions) provided by the TOE.

# 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: the trustworthiness of the certification-generation application and of the signature-creation application. Details can be found in the Security Target [6], chapter 3.1.

The TOE comprises the underlying hardware, the operating system (OS), the SCD/SVD generation, SCD storage and use, and signature-creation functionality.

# 5 Architectural Information

The TOE CardOS V4.2B FIPS with Application for Digital Signature running on Infineon Chips SLE66CX322P and SLE66CX642P is a SSCD implemented by a software (SW) with an application (data structure) for creation of digital signatures running on either the security processor chip hardware (HW) SLE66CX322P m1484 or SLE66CX642P m1485 from Infineon which have already been certified at BSI [17] – [21].

The TOE is divided into the following subsystems: the Protocol Manager, the Command Manager, the Command Layer, the Service Layer, the System Layer, the Resource Management System (RMS), one or more Applications for Digital Signature (ADS) and the underlying chip hardware, Infineon SLE66CX322P / SLE66CX642P.

# 6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

# 7 IT Product Testing

The evaluators have spent effort for the desired resistance of the TOE against attackers with a high attack potential. They analysed the test specification and ensured that the specification has been correctly implemented, they created

independent evaluator tests and ensured that the test environment delivered correct test results.

The developer tests have been compared with the Security Target, the Functional Specification and the High-Level Design. According to EAL4, testing is performed down to a depth of subsystem interfaces.

The TOE tested configuration consists of the configured software (OS, packages and signature application) used to implement the SSCD and the pertaining guidance documentation ‘Administrator Guidance, CardOS V4.2B FIPS’ [11] and ‘User Guidance, CardOS V4.2B FIPS’ [12]. For the tests, modules were used that contain the operating system CardOS V4.2B (mask number C809) in ROM. The application data structure (SigG application as defined by scripts identified in Table 2) has been set using the personalization script files in accordance with [23]. The TOE being tested also contained the packages Command Set Extension Package, CAT Package, DRNG Package, and WIPE Package loaded in the EEPROM as listed in Table 2 above. In addition, the HMAC Package has also been loaded for tests.

# 8 Evaluated Configuration

This certification covers the following configurations of the TOE:

- CardOS V4.2B with FIPS packages and applications based on the Infineon SLE66CX322P Integrated Circuit Card (ICC) platform including HMAC package signature application; Pre-loaded scenario as described in Chapter 2
- CardOS V4.2B with FIPS packages and applications based on the Infineon SLE66CX322P ICC platform including HMAC package signature application; Post-loaded scenario as described in Chapter 2
- CardOS V4.2B with FIPS packages and applications based on the Infineon SLE66CX642P ICC platform including HMAC package signature application; Pre-loaded scenario as described in Chapter 2
- CardOS V4.2B with FIPS packages and applications based on the Infineon SLE66CX642P ICC platform including HMAC package signature application; Post-loaded scenario as described in Chapter 2
- CardOS V4.2B with FIPS packages and applications based on the Infineon SLE66CX322P ICC platform without HMAC package signature application; Pre-loaded scenario as described in Chapter 2
- CardOS V4.2B with FIPS packages and applications based on the Infineon SLE66CX322P ICC platform without HMAC package signature application; Post-loaded scenario as described in Chapter 2
- CardOS V4.2B with FIPS packages and applications based on the Infineon SLE66CX642P ICC platform without HMAC package signature application; Pre-loaded scenario as described in Chapter 2

- CardOS V4.2B with FIPS packages and applications based on the Infineon SLE66CX642P ICC platform without HMAC package signature application; Pre-loaded scenario as described in Chapter 2

All tests have been performed in all possible combinations with and without HMAC package, both personalization scenarios pre-loaded and post-loaded on both chip platforms.

# 9 Results of the Evaluation

## 9.1 CC specific results

The Evaluation Technical Report (ETR), [8] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

For components beyond EAL4 the evaluation methodology applied was defined in co-ordination with the Certification Body [4] (AIS 34).

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

The following guidance specific for the technology was used:

*(i) Functionality classes and evaluation methodology for deterministic random number generators*

*(ii) Application of Attack Potential to Smart Cards*

*(iii) Composite product evaluation*

(see [4], AIS 20, AIS 26, AIS 36) were used.

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

- All components of the class ASE
- All components of the EAL 4 package as defined in the CC (see also part C of this report)
- The components
  AVA_MSU.3 – Analysis and testing for insecure states
  AVA_VLA.4 – Highly resistant
  augmented for this TOE evaluation.

The evaluation has confirmed:

- Conformance to the PP: Protection Profile BSI-PP-0006-2002 [9]
- For the functionality: BSI-PP-0006-2002 conformant
  plus product specific extensions
  Common Criteria Part 2 extended

- For the assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by
  AVA_VLA.4, AVA_MSU.3
- The following TOE Security Functions fulfil the claimed Strength of Function high:

  SF1 – User Identification and Authentication
  SF3 – SCD/SVD Pair Generation
  SF4 – Signature Creation
  SF6 – Secure Messaging
  SF7 – SVD Transfer

  In order to assess the strength of function the scheme interpretations AIS 20 and AIS 26 (see [4]) were used.

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

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
- algorithms for the encryption and decryption:
  - RSA

This holds for the following security functions:

- the TOE Security Function SF3 – SCD/SVD Pair Generation is responsible for the correct generation of the SCD/SVD key pair which is used by the Signatory to create signatures. The TOE generates RSA signature key pairs which fulfill the corresponding requirements of [22] for RSA key pairs.
- the TOE Security Function SF4 – Signature Creation is responsible for signature creation using the SCD of the Signatory. Before a signature is generated by the TOE, the Signatory has to be authenticated successfully. Technically, SF4 generates RSA signatures for hash values with PKCS#1 padding (block type 1) using the SCD of the Signatory.

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 [22] the algorithms are suitable for creation and validation of qualified signatures. The validity period of each algorithm is mentioned in the official catalogue [22] 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 CM/CA shall choose the ICCSN (16 byte unique Integrated Circuit Card Serial Number) in such a way, that both 8 byte strings will differ for different cards. At best, all ICCSN of an arbitrary number of cards will have different last 8 bytes.
- According to the security assessment of the strength of the cryptographic algorithms for qualified electronic signatures given in “Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV” [22], the following time periods for a secure usage of the TOEs algorithms is recommended:
  - For the hash function: SHA-1 until the end of 2009
  - For the TOEs maximum key length: RSA until the end of 2010
- The number of TOE devices (i.e. smart cards) in operational use must not exceed 83 million examples (depending on PIN_DS resp. PUK_DS length, cf. SOF).
- The Initializer and Embedder respectively, and the Certification Authority issuing the TOE smart cards have to ensure that except for the well-defined software defined in Table 2 no other executable code is loaded onto the smart card. It is especially not allowed to load any other or omit loading of mandatory packages than those listed in Table 2, i.e. the Command Set Extension Package, the CAT Package, the DRNG Package and the WIPE Package. The optional HMAC Package can be loaded as well. The CM/CA has to ensure, that misuse of the functionality to load packages is effectively prevented.
- The CM/CA shall use cryptographically strong random number generators for key generation and other aspects (including the challenge-response-authentication).

# 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

| | |
|---|---|
| **APDU** | Application Protocol Data Unit |
| **BSI** | Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany |
| **CCRA** | Common Criteria Recognition Arrangement |
| **CC** | Common Criteria for IT Security Evaluation |
| **CA** | Certification Authority |
| **CM** | Card Manufacturer |
| **EAL** | Evaluation Assurance Level |
| **HMAC** | Keyed-Hashing for Message Authentication |
| **ICC** | Integrated Circuit Card |
| **ICCSN** | Integrated Circuit Card Serial Number |
| **IT** | Information Technology |
| **ITSEF** | Information Technology Security Evaluation Facility |
| **LRA** | Local Registration Authority |
| **PIN_DS** | Digital Signature of the Personal Identification Number |
| **PUK_DS** | Digital Signature of the Personal Unblocking Key |
| **PP** | Protection Profile |
| **SCD** | Signature Creation Data (private key) |
| **SF** | Security Function |
| **SFP** | Security Function Policy |
| **SigG** | Signaturgesetz |
| **SOF** | Strength of Function |
| **ST** | Security Target |
| **SVD** | Signature Verification Data (public key) |
| **TOE** | Target of Evaluation |
| **TSC** | TSF Scope of Control |
| **TSF** | TOE Security Functions |
| **TSP** | TOE Security Policy |

## 12.2 Glossary

**Augmentation** - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

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

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

**Informal** - Expressed in natural language.

**Object** - An entity within the TSC that contains or receives information and upon which subjects perform operations.

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

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

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

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

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

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

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

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

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

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

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

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

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

# 13 Bibliography

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

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

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

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

- AIS 20, Version 2, 2 December 1999 for: CC Supporting Document, - Functionality classes and evaluation methodology for deterministic random number generators
- AIS 26, Version 3, 8 August 2007 for: CC Supporting Document, - Application of Attack Potential to Smartcards, Version 2.1, July, Revision 1, April 2006
- AIS 32, Version 1, 02 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungs-schema.
- AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 36, Version 2, 12 November 2007, Kompositionsevaluierung

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

[6] Security Target BSI-DSZ-0476-2007, Version 1.2, 23.07.2007, CardOS V4.2B FIPS with Application for Digital Signature, Siemens AG

[7] Directive 1999/93/ec of the European parliament and of the council of 13 December on an Community framework for electronic signatures

[8] Evaluation Technical Report, Version 1.02, 10.08.2007, CardOS V4.2B FIPS with Application for Digital Signature, T-Systems GEI GmbH (confidential document)

[9] Protection Profile BSI-PP-0006-2002, Version 1.05, 25.07.2001, CWA 14169:2002 (E)

[10] Configuration list, Chipcard Operating System, CardOS V4.2B FIPS, Version 1.10, 23.07.2007 (confidential document)

[11] Administrator Guidance CardOS V4.2B_FIPS with Application for Digital Signature, Siemens AG, DS1, Version 1.4, Edition 07/2007

[12] User Guidance CardOS V4.2B_FIPS with Application for Digital Signature, Siemens AG, DS1, Version 1.4, Edition 06/2007

[13] CardOS V4.2B_FIPS ADS Description, Version 1.0, Siemens AG, DS1, 05/2007

[14] CardOS V4.2B Chipcard Operating System, CAT, DRNG and WIPE Packages & Release Notes, Version 1.0, Siemens AG, Edition 05/2007

[15] CardOS V4.2B Chipcard Operating System, Packages & Release Notes, Version 1.0, Siemens AG, Edition 05/2007

[16] CardOS V4.2B Chipcard Operating System, User's Manual, Version 1.0, Siemens AG, Edition 09/2005

[17] Certification report for Infineon Smart Card IC (Security Controller) SLE66CX322P with RSA2048/m148418 from Infineon Technologies AG, certification file BSI-DSZ-CC-0266-2005, BSI, 22.04.2005, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[18] Certification report for Infineon Smart Card IC (Security Controller) SLE66CX642P / m1485b16 with RSA 2048 V1.30 and specific IC Dedicated Software from Infineon Technologies, certification file BSI-DSZ-CC-0315-2005, 12.08.2005, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[19] Assurance Continuity Maintenance Report BSI-DSZ-CC-0266-2005-MA-01 for Infineon Smart Card IC (Security Controller) SLE66CX322P/m1484b14 and m1484f18 with RSA 2048 V1.30 and Specific IC Dedicated Software from Infineon Technologies AG, 07.06.2005, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[20] Assurance Continuity Maintenance Report BSI-DSZ-CC-0266-2005-MA-02 for Infineon Smart Card IC (Security Controller) SLE66CX322P/m1484b14 and m1484f18 with RSA 2048 V1.30 and Specific IC Dedicated Software from Infineon Technologies AG, 16.05.2006, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[21] Assurance Continuity Maintenance Report BSI-DSZ-CC-0266-2005-MA-03 for Infineon Smart Card IC (Security Controller) SLE66CX322P/m1484b14 and m1484f18 with RSA 2048 V1.30 and Specific IC Dedicated Software from Infineon Technologies AG, 25.07.2006, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[22] Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV, veröffentlicht am 12. April 2007 im Bundesanzeiger Nr. 69, S.3759, vom 22.Februar 2007, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

[23] CardOS V4.2B FIBS, Application Digital Signature Description, Version 1.00, Edition 05/2007, Siemens AG, 14.05.2007

# 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.

Annex B: Evaluation results regarding development and production environment D-4

This page is intentionally left blank.

# Annex B of Certification Report BSI-DSZ-CC-0476-2007

## Evaluation results regarding development and production environment

The IT product CardOS V4.2B FIPS with Application for Digital Signature running on Infinion Chips SLE66CX322P and SLE66CX642P (Target of Evaluation, TOE) 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 and guidance specific for the technology of the product for conformance to the *Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)*.

As a result of the TOE certification, dated 29. November 2007, the following results regarding the development and production environment apply. The Common Criteria assurance requirements

- **ACM – Configuration management (i.e. ACM_AUT.1, ACM_CAP.4, ACM_SCP.2),**
- **ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.1) and**
- **ALC – Life cycle support (i.e. ALC_DVS.1, ALC_LCD.1, ALC_TAT.1),**

are fulfilled for the development and production sites of the TOE listed below:

a) Siemens AG, Charles de Gaulle Str. 2, D-81737 Muenchen, Germany (Development)

b) Siemens AG, Building East, Von der Tann Str. 31, D-90439 Nuernberg, Germany (Development)

Note, that this evaluation has been performed as a composite evaluation applying the following production sites:

c) Altis Semiconductor S.N.C., Boulevard John Kennedy 224,, 91105 Corbeil Essonnes, France (Production)

d) Infineon Technologies Dresden GmbH & Co. OHG, Königsbrücker Str. 180, 01099 Dresden, Germany (Production)

The chip SLE66CX322P is certified for two production sites: Dresden in Germany (production line indicator ‘2’) and Corbeil Essonnes (called Altis) in France (production line indicator ‘5’)) (see [17], [19] - [21].). The chip SLE66CX642P is certified for the production site Dresden [18].

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target BSI-DSZ-0476-2007, Version 1.2,

23.07.2007, CardOS V4.2B FIPS with Application for Digital Signature, [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6]) are fulfilled by the procedures of these sites.