Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0668-2010

for

CardOS V4.4 with Application for QES

from

Siemens IT Solutions and Services GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0668-2010

Secure Signature Creation Device (SSCD)

CardOS V4.4 with Application for QES

from	Siemens IT Solutions and Services GmbH
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by AVA_VAN.5

Common Criteria Recognition Arrangement for components up to EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 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 3.1.

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, 8 December 2010

For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED

Bernd Kowalski L.S.
Head of Department

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

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 on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

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 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

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 (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic).

The new agreement was initially signed by the national bodies of Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom.

---

2 Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

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 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

Within the terms of this agreement the German Federal Office for Information Security (BSI) recognises

- for the basic recognition level certificates issued as of April 2010 by the national certification bodies of France, The Netherlands, Spain and the United Kingdom.
- for the higher recognition level in the technical domain Smart card and similar Devices certificates issued as of April 2010 by the national certification bodies of France, The Netherlands and the United Kingdom.

In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

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

Historically, the first SOGIS-Mutual Recognition Agreement Version 1 (ITSEC only) became initially effective in March 1998. It was extended in 1999 to include certificates based on the Common Criteria (MRA Version 2). Recognition of certificates previously issued under these older versions of the SOGIS-Mutual Recognition Agreement is being continued.

2.2 International Recognition of CC – Certificates (CCRA)

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 January 2009 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, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and 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 component AVA_VAN.5 that is not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition, the EAL4 components of this assurance family is 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 V4.4 with Application for QES has undergone the certification procedure at BSI. The evaluation was not carried out as a re-evaluation. However, certain aspects of the certification process BSI-DSZ-CC-0476-2007 were taken into consideration and used for reasoning.

The evaluation of the product CardOS V4.4 with Application for QES was conducted by T-Systems GEI GmbH. The evaluation was completed on 28 October 2010. 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 IT Solutions and Services GmbH.

The product was developed by: Siemens IT Solutions and Services GmbH.

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 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 evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

5 Publication

The product CardOS V4.4 with Application for QES 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.

This page is intentionally left blank.

---

6 Information Technology Security Evaluation Facility

7 Siemens IT Solutions and Services GmbH
Otto-Hahn-Ring 6
81739 München
Deutschland

This page is intentionally left blank

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 "CardOS V4.4 with Application for QES" is a smartcard that is to be used as a Secure Signature Creation Device (SSCD). The smart card is based on the Infineon Chip SLE66CX680PE. The TOE allows to generate electronic signatures over previously externally calculated hash values. The TOE generates the signature key pair. It is able to protect the secrecy of the internally generated and stored Signature Creation Data (SCD, i.e. secret key) and restricts the usage access to the authorised signatory only. The restriction on the access to the secret key is done via a PIN authentication mechanism.

The Security Target [6] is the basis for this certification.

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 4 augmented by AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed issue
SS1	User Identification and Authentication
SS2	Access Control
SS3	SCD/SVD Pair Generation
SS4	Signature Creation
SS5	Protection

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.1.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3. 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 3.1 to 3.3.

This certification covers the “CardOS V4.4 with Application for QES”. There are some parameters that can be set to one or another value which results in different configurations, for details refer to chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

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 V4.4 with Application for QES

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	Software (Operating System)	CardOS V4.4	C80D, 23.06.09	loaded in ROM / EEPROM
2	V4.4 Software Application, Digital Signature (Application / Data Structure)	*Centralized Model:*		Personalization Script Files in CSF format, after whose execution the ADS will be loaded in EEPROM
		PersAppSigG.CSF	#4(*), 27.05.10	
		PersAppSigG_withoutPUK.CSF	#4(*), 27.05.10	
		De-Centralized Model:		
		Pre-PersAppSigG.CSF	#4(*), 27.05.10	
		Post-PersAppSigG.CSF	#4(*), 27.05.10	
		Pre-PersAppSigG_withoutPUK.CSF	#4(*), 27.05.10	
		Post-PersAppSigG_withoutPUK.CSF	#4(*), 27.05.10	
		Mass_Pre-PersAppSigG.CSF	#4(*), 27.05.10	
		Mass_Post-PersAppSigG.CSF	#4(*), 27.05.10	
		Both Models:		
		Defines_1024.csf	#3(*), 27.05.10	
		Defines_1280.csf	#3(*), 27.05.10	
		Defines_1536.csf	#3(*), 27.05.10	
		Defines_1792.csf	#3(*), 27.05.10	
		Defines_2048.csf	#3(*), 27.05.10	
3	Service Package (mandatory)	Service Package	03h 04h 13h 01h C8h 0Dh(**) 26.05.10	Personalization Script Files in CSF format, after whose execution the resp. code will be loaded in EEPROM (included in the (Pre-) Pers-CSF-Scripts above)
4	Software Verify_RC Package (mandatory)	Verify_RC Package	03h 04h 02h 01h C8h 0Dh(**) 26.05.10	
5	Software SHA-2 Package (optional)	SHA-2 Package	03h 04h 05h 03h C8h 0Dh(**) 22.12.09	
6	Documentation	CardOS License Package Tool Manual [19]	1.3, 09/2005	Paper form or PDF-File
7	Documentation	CardOS V4.2B User's Manual [14]	1.0, 09/2005	
8	Documentation	CardOS V4.4 Packages & Release Notes [15]	2.0, 05/2010	

No	Type	Identifier	Release	Form of Delivery
9	Admin Documentation	CardOS V4.4 Administrator Guidance [11]	0.40, 04/2010	
10	User Documentation	CardOS V4.4 User Guidance [12]	0.40, 04/2010	
11	ADS Documentation	CardOS V4.4 ADS_Description [18]	0.40, 04/2010	
12	Hardware (Chip)	Infineon SLE66CX680PE	m1534-a14 (Dresden)	Module
13	Firmware RMS	RMS	RMS V2.5	Stored in reserved area of User ROM
14	Software crypto library	RSA2048 crypto library	Version 1.5	Loaded in ROM
15	Firmware STS	Self Test Software	V55.0B.07	Stored in Test ROM

Table 2: Deliverables of the TOE

(*) Last two characters of entry %VERSION%

(**) PID (package ID) containing package version

2.1 Overview of the delivery procedure

The delivery from the TOE software developer (SW-DVL) to the chip manufacturer (CPM) is outlined in section 4.3 of [16] and the delivery to the trust center / certification authority (TC/CA) is outlined in section 4.4 of [16] including the general processing chain. The delivery to the card holder (CH) is explained in section 4.5 of [16]. The delivery of the terminal developer (TD) is described in section 4.6 of [16].

The trust center / certification authority (TC/CA) receives the TOE specific hardware from the CPM and the software and documentation parts of the TOE from the SW-DVL.

The TC/CA is responsible for handling the TOE (hardware, software and documentation) in such a way that its confidentiality, integrity and authenticity are guaranteed in the domain of TC/CA.

Before finally reaching the card holder (CH), the manufactured hardware passes the following logical entities whose work items may or may not be executed by separate organizational entities (e.g. in the domain of one TC):

- Embedder (EMB): Initialisation
- Certification Authority (CA): Key generation
- Personalizer (PERS): Personalization
- (Local) Registration Authority (LRA): Certificate installation

All these entities (EMB, CA, PERS, LRA) are compelled to accept the security policy formulated and enforced by TC/CA. The TC/CA security policy should assert that each entity applies the acceptance procedure detailed in the TOE's administrator guidance and that modification of the incomplete hardware is only possible after authentication with an entity specific authentication key.

The delivery from the TC/CA to the card holder is subject to the TC/CA security policy, too. The SW-DVL never interacts with the CH (the end user) directly. Therefore, there is no direct interface between SW-DVL and CH.

The delivery from the TC/CA to the terminal developer (TD) is subject to the TC/CA security policy, too.

2.2 Identification of the TOE by the end user

The end user (card holder) can identify his signature card by reading out i) the card name and version, ii) information about the loaded packages, and iii) information about the chip.

This information can be retrieved by using the following steps (xyh stands for a byte xy in hexadecimal notation, x and y are variables):

- The version of the operating system can be identified with the command GET DATA using specific modes (see [14], chapter 3.20):
  Mode 82h must return the OS version "C8h 0Dh "
  Mode 80h must return the product name, version and copyright string “CardOS V4.4 (C) Siemens AG 1994-2009." (43h 61h 72h 64h 4Fh 53h 20h 56h 34h 2Eh 34h 20h 28h 43h 29h 20h 53h 69h 65h 6Dh 65h 6Eh 73h 20h 41h 47h 20h 31h 39h 39h 34h 2Dh 32h 30h 30h 39h 00h).
- Information about loaded packages can be checked with the command GET DATA using mode 88h (see [14], chapter 3). Its response has to show the mandatory Service Package:
  E1h 09h 03h 04h 13h 01h C8h 0Dh 8Fh 01h 01h,
  the mandatory package Verify_RC:
  E1h 09h 03h 04h 02h 01h C8h 0Dh 8Fh 01h 01h
  and may show the optional package SHA-2:
  E1h 09h 03h 04h 05h 03h C8h 0Dh 8Fh 01h 01h.
- Identification of the chip (hardware, RMS, crypto library, STS) can be done via GET DATA in mode 81h (see [14], chapter 3.20), that must show 32 bytes whereby the ninth byte (first index equals 1) contains the chip type,
  which must be 91h for the SLE66CX680PE,
  and the eleventh byte the production line:
  2xh for Dresden.

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 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:

- OE.CGA_QCert: Generation of qualified certificates
- OE.SVD_Auth_CGA: CGA verifies the authenticity of the SVD
- OE.HI_VAD: Protection of the VAD
- OE.SCA_Data_Intend: Data intended to be signed
- OE.SCA_Trusted_Env: Trusted environment
- OE.Env_KeyGen: Generation of SCD/SVD key pairs

Details can be found in the Security Target [6], chapter 4.2.

5 Architectural Information

The TOE (CardOS V4.4 with Application for QES) 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 [17].

The TOE consists of i) configured software (OS, packages and signature application) ii) the underlying hardware (SLE66CX680PE from Infineon) used to implement the secure signature-creation device (SSCD) and iii) the pertaining guidance documentation.

The operating system (the CardOS V4.4, mask number C80Dh) is loaded into the ROM, all packages are loaded in EEPROM and the application data structure is created by personalization script files.

The external physical interface of the smart card is given by a contact field for data exchange. The TOE provides a logical interface being used to exchange commands and responses between each IFD (interface device) and the TOE by transferring APDUs (application protocol data unit).

The software description and instruction set of the CardOS V4.4 operating system can be found in the “User’s Manual CardOS V4.2B” [14]. Additional information (e.g. modes of operation and application specific command sequences) are given in “CardOS V4.4, User Guidance” [12], and in the “CardOS V4.4, Administrator Guidance” [11].

The TOE is divided into the following eight subsystems:

Subsystem 1: Protocol Manager (monitors the correct data transfer)

Subsystem 2: Command Manager (implements the command identification)

Subsystem 3: Command Layer (contains the interpretation of all CardOS commands)

Subsystem 4: Service Layer (contains service and security routines)

Subsystem 5: System Layer (contains system and basic routines)

Subsystem 6: RMS v2.5 (contains writing routines for EEPROM, RNG tests, toggeling the VPLL and analysing of error codes)

Subsystem 7: ADS (application digital signature, DF_SigG)

Subsystem 8: IC (SLE66CX680PE secure micro controller)

For the implementation of the TOE Security Functions basically the components mentioned above are realized within the software with the exception of subsystem 8 which comprises the underlying IC and is therefore a hardware implementation.

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

7.1 Test and penetration concept

The evaluators have spent adequate testing effort for the desired resistance of the TOE against attackers with a high attack potential. The evaluators spent several days each

- for analysing the test specification and ensuring that the specification has been correctly implemented in the test scripts,
- for creating ideas for independent evaluator tests,
- for ensuring that the test environment delivers correct test results and then for repeating developer tests as well as carrying out independent tests.

Due to the test set-up, it was rather easy to check that the actual test results match the expected test results, simply by searching full-text through the test protocol.

The following testing approach was chosen: Independent tests were identified based on the developer tests already available. The developer tests have been compared with the ST, the FSP and the TDS in order to determine the fields of further investigation.

According to EAL4, testing is performed down a depth of subsystem interfaces. Since

- the product type of the TOE is a smart card, the interfaces of which are most easily accessible through the TSFI (command APDUs and response APDUs), and since
- testing via command APDUs provides additional advantages like easy repeatability (re-run scripts) and protocol files (by logging the APDU traffic sent to and received from the TOE),

the evaluators tried to perform as many test cases as possible through implementing test scripts. However, the need arose to test effects that are not visible through the TSFI. For such effects, tests using the simulator or the emulator have been carried out, which allowed to selectively inspect and even manipulate memory content, to set breakpoints and even to follow the program control flow in single step mode.

The tests showed that the TOE behaves as expected in all configurations that are considered as part of the evaluation. The depth of testing is adequate for the evaluation assurance level chosen (EAL4+). The TOE has successfully passed independent testing.

7.2 Description of test configuration

The tested TOE configuration consists of the configured software (OS, packages and signature application) used to implement the secure signature-creation device (SSCD). The software runs on the security processor chip SLE66CX680PE from Infineon.

For the tests, the operating system CardOS V4.4 (mask number C80Dh) resides in the ROM. The application data structure is set using the personalization script files. The TOE being tested also contained the packages Service Pack, Verify_RC and SHA256 package loaded in the EEPROM.

The Application for QES can be personalized in two different ways, which are named ‘Centralized model’ and ‘De-centralized model’. Apart from that, different configurations within the models are possible. The variants are determined through the use of the appropriate personalization scripts or through other personalization processes that guarantee the same result.

The following parameters can be set to one or another value:

- DSI-object is optional,
- PUK-object is optional,
- If the PUK-object exists, it can be delivered deactivated (standard case) or activated (‘PUK-letter concept’).

Besides this, the TOE can be personalised (whatever the personalisation mode is) as one of the following different signature creation devices:

- Configuration ‘one PIN’ + ‘normal SSCD’
  (I) using one PIN object with associated ARA_Counter ARA_Cnt = 1: user authentication expires after generating exactly one signature;
- Configuration ‘one PIN’ + ‘mass signature SSCD’
  (ii) using one PIN object with associated ARA_Counter ARA_Cnt between 2 and 254: user authentication expires after generating ARA_Cnt number of signatures;
  (iii) using one PIN object with associated ARA_Counter ARA_Cnt {0h, FFh}: user authentication never expires within the current security context,
- Configuration ‘two PINs’ + ‘mass signature SSCD’
  (iv) using two PIN objects with associated ARA_Counter ARA_Cnt having a deliberate value between 0 and 255. In this case, user authentication function checks the logical test object (PIN1 AND PIN2). However, due to the special property of the TOE the value of the associated ARA_Counter is ignored and, hence, user authentication never expires within the current security context. This variant of ‘mass signature module’ implementation is called ‘Two PIN’-Module by the developer.

There are two different personalisation ways – central and decentral personalisation –, which represent, speaking the language of the CC, different delivery and configuration procedures. The final TOE in its operational phase resulting from these personalisation procedures is the same object from the point of view of its security and functional behaviour.

The developer has tested the final TOE with all possible parameters and personalised according to both personalisation procedures.

Most of the testing effort is realised by using automated script based tests. For these tests the complete interaction with the TOE is given by the communication resp. the data traffic (APDUs) transmitted over a card terminal. All security services, except SS5, are completely addressed via this APDU interface.

Some tests addressing the SS5 focus also on the interaction with the chip surface (hardware) and internal security mechanisms that cannot be directly addressed by using APDUs. These test procedures comprise manual test and emulator tests allowing to affect the TOE in a way that is not intended by the 'ordinary' interfaces (e.g. object reuse, reaction on checksum errors).

The test strategy was to test the single properties of the security enforcing functions (their behaviour). The single test cases (noted by unambiguous test-IDs) were produced and performed for each external visible interface of each security service. The manual tests covered the special properties of the security services having been not testable via the external interfaces.

The test scripts implementing the automated tests contained also the expected test results. The test environment of the developer reported of each deviation between the expected and actual test results, so that the developer was able to search for, to find and to correct all errors, if any.

The tests implemented by the developer include tests of all APDUs being relevant for the TSF with their characteristic input parameters. This ensures coverage of the TSF in a sense like ATE_COV.

The SS5 (Protection) and some other special properties of the TSFs (e.g. decrementing of the retry counter or clearing of residual RAD/VAD data) could not be tested based on APDUs only; for this TSF special tests have been carried out on a simulator or emulator.

All in all, the developer tests covered all security functions defined in the Security Target. Where possible, the tests were performed at the APDU level, ensuring coverage of at least all TSF interfaces (TSFI). Since there is a direct mapping between APDUs and modules, the testing depth is on TDS level.

The test specification comprises over 200 test cases, the test logs in ASCII format comprise around 30 MB. Overall, the developer testing results showed that the TOE behaves as expected, i.e. as specified in the ADV documentation.

7.3 Penetration testing

Potential vulnerabilities were identified in the evaluator's vulnerability analysis. However, the analysis shows that none of these potential vulnerabilities is exploitable by an attacker, even with high attack potential.

The penetration tests have been performed using real cards, test cards and using the emulator. Both, the centralised and the decentralised personalisation model, have been tested. Where there was a difference in the behaviour, the preconditions for each test are listed in the respective documentation. Tests have also been performed with various key lengths, focusing on the most commonly used key lengths, but testing also other modulus lengths, including modulus lengths with an odd number of bytes.

8 Evaluated Configuration

This certification covers the following configuration of the TOE: CardOS V4.4 with Application for QES.

CardOS V4.4 with Application for QES supports two personalization schemes for the TOE:

- the centralized model, where the key generation, the generation of the certificate and the storage of the personalization data all take place only in the TC, and
- the decentralized model, where the certificate request and the storage of the personalization data take place in an RA, which is locally separated from the CA.

Apart from that, different configurations within the models are possible. The variants are determined through the use of the appropriate personalization scripts or through other personalization processes that guarantee the same result. The following parameters can be set to one or another value:

- Both models:
  - The PUK and the DSI Object are optional in the DF_SigG.
  - The PUK is needed only if unblocking of the PIN shall be possible.
- Centralized model: The certificate(s) are optional in the DF_SigG. If the certificate(s) are stored in the DF_SigG they cannot be updated later and no Issuer_CR_Key is needed for the signature application. If the Issuer_CR_Key does not exist, all access conditions set to this key must instead be set to never.
  If the certificate(s) are stored in a separate DF, the Issuer_CR_Key is mandatory for a later update.
- Decentralized model: The certificate(s) have to be stored in a separate DF (MF) and can be updated later after an authentication with the mandatory Issuer_CR_Key.
  Concerning management of pre-personalized cards either a model using a central database or a model using transport certificates has to be chosen. If the transport certificate variant is used, the transport certificate will be stored in a container that will later on be used for storage of the card holder's certificate for qualified electronic signatures.
  - Unlimited mass signature module (Only decentralized model):
    Two PIN Sets belonging to two different persons (Signatory and PIN_2 Owner).
    PIN Set 1 = PIN_1, PUK_1, Transport PIN_1 (Signatory)
    PIN Set 2 = PIN_2, PUK_2, Transport PIN_2 (PIN_2 Owner)
    If PUK functionality shall not be provided, USECOUNT of PUKs must be set to zero.

For identification of the TOE, please refer to Chapter 2.2 of this report.

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.

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 (AIS 34) and guidance specific for the technology of the product [4].

The following guidance specific for the technology was used:

- As the evaluation of the TOE was conducted as a composition evaluation, the ETR [8] includes also the evaluation results of the composite evaluation activities in accordance with CC Supporting Document, ETR for Composition: Annex A Composite smart card evaluation [4, AIS 36].
- The ETR [8] builds up on the ETR for Composition documents of the evaluation of the underlying hardware "SLE66CX680PE / m1534-a14 with RSA2048_V1.5 from Infineon Technologies AG" ([9]).
- For smart card specific methodology the scheme interpretations AIS 25 and AIS 26 (see [4], AIS 25, AIS 26) were used.

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

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The component AVA_VAN.5 augmented for this TOE evaluation.

The evaluation was not carried out as a re-evaluation. However, certain aspects of the certification process BSI-DSZ-CC-0476-2007 were taken into consideration and used for reasoning.

The evaluation has confirmed:

- for the Functionality: Product specific Security Target
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by AVA_VAN.5

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:

- algorithms for the encryption and decryption:

  RSA

This holds for the following security functionalities:

- SS3 SCD/SVD Pair Generation and SS4 Signature Creation

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). According to [20] the algorithms are suitable for creation and validation of qualified signatures. The validity period of each algorithm is mentioned in the official catalogue [20] 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 all aspects of Assumptions, Threats and Policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process.

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

- The software developer (Siemens IT Solutions and Services GmbH) and the chip manufacturer (Infineon Technologies AG) are responsible to prevent misuse of the PackageLoadKey; especially they have to ensure the confidentiality of this key.
- The TOE configuration mass signature generation must be permitted only to be used if the TOE has been personalised to be operated under an appropriate external security policy. It does not mean any confinement of institution enforcing such a security policy. For example, such a security policy is often applied by a Trust Centre for its services, e.g. like a time stamp. The fulfilment of this stipulation is in the responsibility of the Trust Centre issuing the TOE.
- Besides the general recommendations concerning the quality of a PIN/PUK (e.g. length, retry count, etc.) as stated in the user guidance [12], sec. 2.1, the user must be urged to choose a non trivial PIN/PUK before using the TOE in its operational state.
- From the beginning of 2011 on the length of modulus for RSA are restricted to at least 1976 Bit. This recommendation is valid at least up to the year 2016 [20].

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

ADS Application Digital Signature

AIS Application Notes and Interpretations of the Scheme

APDU Application Protocol Data Unit

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

BSIG BSI-Gesetz / Act on the Federal Office for Information Security

CA Certification authority

CCRA Common Criteria Recognition Arrangement

CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CGA	Certification Generation Application
CH	Card Holder
CPM	Chip Manufacturer
CSP	Certification Service Provider
DOC	Documentation / documents
DTBS	Data to be signed
EAL	Evaluation Assurance Level
EEPROM	Electronically Erasable Programmable Read Only Memory
EMB	Embedder
ETR	Evaluation Technical Report
FSP	Functional Specification
HW	Hardware
IC	Integrated Circuit
ID	Identification Number
IFD	Interface Device
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
LRA	Local Registration Authority
OS	Operating System
PERS	Personalizer
PIN	Personal Identification Number
PP	Protection Profile
PUK	Personal Unblocking Key
QES	qualifizierte elektronische Signatur, qualified electronic signature
RA	Registration Authority
RNG	Random Number Generator
ROM	Read Only Memory
RSA	Rivest-Shamir-Adleman Algorithm
SAR	Security Assurance Requirement
SCA	Signature creation application
SCD	Signature Creation Data (private key)
SFP	Security Function Policy

SFR	Security Functional Requirement
SigG	Signaturgesetz
SSCD	Secure Signature Creation Device
SSCR	Self Signed Certificate Request
ST	Security Target
SVD	Signature Verification Data
SW	Software
SW-DVL	Software developer
TC	Trust Center
TD	Terminal Developer
TDES	Triple DES
TDS	TOE Design Specification
TOE	Target of Evaluation
TSF	TOE Security Functionalities
VAD	Verification Authentication Data

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a 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 passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

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

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - A set of software, firmware and/or hardware possibly accompanied by guidance.

TOE Security Functionality - combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 1, September 2006
Part 2: Security functional components, Revision 2, September 2007
Part 3: Security assurance components, Revision 2, September 2007

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 2, September 2007

[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), periodically updated list, published also on the BSI Website

[6] Security Target, CardOS V4.4 with Application for QES, Version 0.50, Edition 04/2010, Siemens AG, 29.04.2010

[7] Certification report for SLE66CX680PE / m1534-a14, SLE66CX360PE / m1536-a14, SLE66CX482PE / m1577-a14, SLE66CX480PE / m1565-a14, SLE66CX182PE / m1564-a14, all optional with RSA2048 V1.5 and all with specific IC dedicated software, from Infineon Technologies AG, Certification ID BSI-DSZ-CC-0437-2008, 27.05.2008, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[8] Evaluation Technical Report, BSI-DSZ-CC-0668, Version 1.03, 27 October 2010, T-Systems GEI GmbH (confidential document)

[9] ETR for composite evaluation according to AIS 36 for the Product SLE66CX680PE / m1534-a14 with RSA2048_V1.5 from Infineon Technologies AG, Certification ID BSI-DSZ-CC-0437, Version 4, TÜV Informationstechnik GmbH, 27.04.2010 (confidential document)

[10] CardOS V4.4 with Application for QES Configuration List 10/2010, V. 0.1, Siemens IT Solutions and Services GmbH, 06.10.2010 (confidential document)

[11] CardOS V4.4, Administrator Guidance, Edition 04/2010, Version 0.40, Siemens AG, 29.04.2010

[12] CardOS V4.4, User Guidance, Edition 04/2010, Version 0.40, Siemens AG, 29.04.2010

[8] specifically

- AIS 25, Version 6, 7 September 2009, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 7, 3 August 2010, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 32, Version 6, 3 August 2010, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 2, 24 October 2008, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 36, Version 3, 19 October 2010, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[13] Sequences of the personalisation scripts, Siemens AG, CardOS V44 SigG Personalization scripts dated 27.05.2010

[14] User's Manual CardOS V4.2B, release 09/2005, Siemens AG, 09.2005

[15] CardOS V4.4, Package & Release Notes, Siemens AG, Edition 05/2010

[16] CardOS 4.4 (CNS) and CardOS DI V4.2C CNS, Life-cycle support, Siemens AG, Version 0.30, Edition 02/2010, 20.01.2010

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

[18] CardOS V4.4, ADS Description, Edition 04/2010, Version 0.40, Siemens AG, 29.04.2010

[19] CardOS License Package Tool Manual, 1.3, 09/2005, Siemens AG

[20] 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 04. Februar 2010 im Bundesanzeiger Nr. 19, S. 426, Vom 06. Januar 2010, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

C Excerpts from the Criteria

CC Part1:

Conformance Claim (Chapter 9.4)

„The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - CC Part 3 extended - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-

Assurance Class	Assurance Components
	level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
ATE: Tests	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“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 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC 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 augmented with extended assurance requirements.”

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“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 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

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.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“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 practise. 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 8.5)

“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 practises.

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 8.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises 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 8.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises 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 8.8)

“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 8.9)

“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.”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

This page is intentionally left blank

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 39

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0668-2010

Evaluation results regarding development and production environment

The IT product CardOS V4.4 with Application for QES (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 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 3.1.

As a result of the TOE certification, dated 8 December 2010, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ALC_TAT.1)

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

a) Siemens IT Solutions and Services GmbH, Otto-Hahn-Ring 6, 81739 Munich, Germany (Software development, Testing, CMS, TOE (i.e. MASK) generation, Documentation)

b) Siemens IT Solutions and Services GmbH, Allee am Röthelheimpark 3A, 91052 Erlangen, Germany (Software development)

c) For development and production sites regarding the “SLE66CX680PE / m1534-a14 with RSA2048_V1.5 from Infineon Technologies AG“ refer to the certification report BSI-DSZ-CC-0437-2008.

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [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.

This page is intentionally left blank.