Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0833-2013

for

CardOS V5.0 with Application for QES, V1.0

from

Atos 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-0833-2013

Digital signature: Secure Signature Creation Devices (SSCD)

CardOS V5.0 with Application for QES, V1.0

from	Atos IT Solutions and Services GmbH
PP Conformance:	None
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 5 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, 26 July 2013

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

---

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

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

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

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 September 2011 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 website: 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 by the nations listed above.

This evaluation contains the components AVA_VAN.5 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 V5.0 with Application for QES, V1.0 has undergone the certification procedure at BSI.

The evaluation of the product CardOS V5.0 with Application for QES, V1.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 25 July 2013. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant is: Atos IT Solutions and Services GmbH.

The product was developed by: Atos 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

[6] Information Technology Security Evaluation Facility

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

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product CardOS V5.0 with Application for QES, V1.0 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[7] Atos 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 the product CardOS V5.0 with Application for QES, V1.0 provided by Atos IT Solutions and Services GmbH. The TOE is a smart card integrated circuit product with the CardOS operating system and a Digital Signature Application, based on the Infineon Chips SLE78CFX*P (M7892 B11: SLE78CFX2400P with 240kByte flash, SLE78CFX3000P with 300kByte flash or SLE78CFX4000P with 404kByte flash).

In general, the TOE is intended to be used as Secure Signature Creation Device (SSCD) for qualified electronic signatures in accordance with the European Directive 1999/93/EC. The related Protection Profile [21] has been used as a baseline, but with specific deviations/additions. Specific configurations of the TOE can be used in order to fulfil the requirments of the laws on digital signatures in Germany and Switzerland.

The TOE allows to generate electronic signatures over previously externally or internally calculated hash values. The TOE generates a signature key pair (Signature Creation Data SCD and Signature Verification Data SVD) based on RSA with a key length of up to 4096 bit. It is able to protect the secrecy of the internally generated and stored SCD (i.e. secret key) and restricts the usage access to the authorized Signatory only. The restriction on the access to the secret key is done via the well-known PIN authentication mechanism.

During initialisation and personalisation phase the TOE can be configured in three different ways:

- the TOE can generate single signatures (i.e. re-authentication before each signature) that fulfil the requirements for Qualified Electronic Signatures (QES) of Germany or Switzerland (variants “QES-Germany” or “QES-Switzerland”)
- the TOE can generate limited (2-255) or an unlimited number of signatures in a row (without intermediate re-authentication) that fulfil the requirements for Qualified Electronic Signatures (QES) of Germany or Switzerland (variants “QES-Germany” or “QES-Switzerland”)
- the TOE can generate an unlimited number of signatures, but secured by two PINs (four-eyes principle, variant “QES-Two-PIN-Signatures”).

The TOE CardOS V5.0 with Application for QES, V1.0 was evaluated in all of its three configurations as described in the ST:

- QES-Germany (according to [18] for single and mass signatures without four eyes principle (4EP))
- QES-Switzerland (according to [20] for single and mass signatures without four eyes principle)
- QES-Two-PIN-Signatures (similar to [18], for mass signatures with four eyes principle)

In order to reflect the differences of the configurations, three sets of SFRs were made up for the TOE. The SFRs were broken down in five parts:

SFRs		**QES-Germany**	**QES-Switzerland**	**QES-Two-PIN-Signatures**
Part ONE	general SFRs	X	X	X

SFRs		QES-Germany	QES-Switzerland	QES-Two-PIN-Signatures
Part TWO	SFRs according to signatures without four eyes principle	X	X	
Part THREE	SFRs based on German QES	X		X
Part FOUR	SFRs according to Swiss QES only		X	
Part FIVE	SFRs according to signatures with four eyes principle			X

Table 1: SFRs of the three TOE configurations

The TOE can be delivered in three different IC sizes: On IC SLE78CFX2400P (240 kByte flash), SLE78CFX3000P (300 kByte flash) or SLE78CFX4000P (240kByte flash), that are all certified under the same certification ID for the M7892 B11 (BSI-DSZ-CC-0758-2012).

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 8.2. The SFRs as defined in the Protection Profile for Secure signature creation device - Part 2: Device with key generation [21] have been used as a baseline. The SFR 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 Functions	Addressed issue
SS1	User Identification and Authentication
SS2	Access Control
SS3	SCD/SVD Pair Generation
SS4	Signature Creation
SS5	Protection

Table 2: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 10.1.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 5. Based on these assets the TOE Security Problem is defined in terms of Assumptions,

Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 5.1 to 5.4.

This certification covers the CardOS V5.0 with Application for QES, V1.0. 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 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 V5.0 with Application for QES, V1.0,

The following table outlines the TOE deliverables:

- the configured software (OS "CardOS V5.0", the service package (patches), personalization script files and signature application),
- the underlying hardware (SLE78CFX*P[8] (M7892 B11) from Infineon) used to implement the secure signature-creation device (SSCD), and
- the pertaining guidance documentation

No	Type	Identifier	Release Version	Release Date	Form of Delivery
1	Hardware (chip)	SLE78CFX*P (M7892 B11)	M7892 B11	-	IC package
2	Software	CardOS for 240kByte flash	C901	2012-05-16	loaded in protected part of Flash EEPROM
3	Software	CardOS for 300kByte flash	C901	2012-05-16	loaded in protected part of Flash EEPROM
4	Software	CardOS for 404kByte flash	C901	2012-05-16	loaded in protected part of Flash EEPROM
5a	Software	RSA-library	1.02.013	-	loaded in protected part of Flash EEPROM

[8] The term SLE78CFX*P stands as wildcard for the three sizes SLE78CFX2400P, SLE78CFX3000P or SLE78CFX4000P

No	Type	Identifier	Release Version	Release Date	Form of Delivery
5b	Software	Toolbox	1.02.013	-	loaded in protected part of Flash EEPROM
5c	Software	SHA-2-library	1.01	-	loaded in protected part of Flash EEPROM
6	Personalization script for QES Germany centralized model	PersAppSigG.csf	#2	2013-03-19	file
7	Pers. script for QES Germany centr. Model without PUK	PersAppSigG_withoutPUK.csf	#2	2013-03-19	file
8	Pers. script for QES Germany decentralized model, file system only (by Trust Center)	Pre-PersAppSigG.csf	#2	2013-03-19	file
9	Pers. script for QES Germany decentralized model, end user data + certificate (by RA)	Post-PersAppSigG.csf	#2	2013-03-19	file
10	Pers. script for QES Germany decentr. model, file model only (by TC), without PUK	Pre-PersAppSigG_withoutPUK.csf	#2	2013-03-19	file
11	Pers. script for QES Germany decentr. model, end user data + certificate (by RA), without PUK	Post-PersAppSigG_withoutPUK.csf	#2	2013-03-19	file
12	Pers. script for QES similar to QES Germany decentr. model, file system only (by TC), for 4EP mass signature	Mass_Pre-PersAppSigG.csf	#2	2013-03-19	file

No	Type	Identifier	Release Version	Release Date	Form of Delivery
13	Pers. script for QES similar to QES Germany decentr. model, end user data + certificate (by RA), for 4EP mass signature	Mass_Post-PersAppSigG.csf	#2	2013-03-19	file
14	Constants definitions for RSA key pair, length 1976 bits, centr. and decentr. mode	Defines_1976.csf	#2	2013-03-19	file
15	Constants definitions for RSA key pair, length 2048 bits, centr. and decentr. model	Defines_2048.csf	#2	2013-03-19	file
16	Constants definitions for RSA key pair, length 2560 bits, centr. and decentr. model	Defines_2560.csf	#2	2013-03-19	file
17	Constants definitions for RSA key pair, length 3072 bits, centr. and decentr. model	Defines_3072.csf	#2	2013-03-19	file
18	Constants definitions for RSA key pair, length 3584 bits, centr. and decentr. model	Defines_3584.csf	#2	2013-03-19	file
19	Constants definitions for RSA key pair, length 4096 bits, centr. and decentr. model	Defines_4096.csf	#2	2013-03-19	file
20	Service Package	V50_ServicePack_Package.csf	1	2013-03-19	file
21	Documentation	User Guidance 'CardOS V5.0 with Application for QES V1.0'	1.40	2013-03-27	paper or PDF file
22	Documentation	CardOS V5.0 Package & Release Notes	-	03/2013	paper or PDF file

No	Type	Identifier	Release Version	Release Date	Form of Delivery
23	Documentation	Administrator Guidance 'CardOS V5.0 with Application for QES V1.0'	1.30	2013-03-27	paper or PDF file
24	Documentation	CardOS V5.0, User's Manual	-	03/2013	paper or PDF file
25	Documentation	Application Digital Signature 'CardOS V5.0 with Application for QES V1.0'	1.10	2013-03-27	paper or PDF file

Table 3: Deliverables of the TOE

2.1 TOE Delivery

The items #1 to #5 are actually delivered as one item (IC platform containing the software mask) to the customer trust center as the flash loading takes place in the production environment at Infineon.

The three items #2, 3 and 4 represent the OS software mask, which is available in three different sizes according the IC size they are used on. The SW image is firstly built as generic mask and is then used to generate these custom-sized masks with the Infineon Post Locater tool. These mask files are delivered to Infineon. The flash loader is deactivated when the Infineon chip leaves the production site.

The items number #6 to #19 in the table above represent the personalisation script files, which are required to prepare the TOE at the trust center and to initialize and personalize it. The three different configurations (QES-Germany, QES-Switzerland and QES-Two-PIN-Signatures) are generated with the help of these personalisation scripts in the preparation phase by the trust center. All files are delivered to the trust center. Its further use for generating the TOE and its different configurations is described in the guidance for administration [11] chp. 4.2.

The preparation of the TOE can be processed by two different scenarios: The decentralized model and the centralized model:

- Centralized model: Initialization and personalization take place only in the Trust Center,
- Decentralized model: Initialization takes place in the Trust Center and personalization takes place in the Registration Authority, which is locally separated from the Certification Authority.

The trust center / certification authority (TC/CA)

- receives the TOE specific hardware including the embedded software (items #1 - #5) from the Chip Manufacturer (by courier or direct by collection at the Infineon Site) and
- receives the script files and documentation (items #6 to #25) from the SW-DVL Atos IT Solutions and Services GmbH as signed and encrypted files.

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 according to the guidance documentation.

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

Delivery of the script files and documentation (items #6 to #25) from the TC/CA to those separate entities has to be as signed and encrypted files, too.

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 card holder (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. Delivery of the related documentation (items #24) from the TC/CA to the TD has to be as signed and encrypted files.

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 [13], chapter 3.23):
  Mode 82h must return the OS version "C9h 01h "
  Mode 80h must return the product name, version and year: “CardOS V5.0, 2012."
  (43h 61h 72h 64h 4Fh 53h 20h 56h 35h 2Eh 30h 2Ch 20h 32h 30h 31h 32h 00h).
- Information about loaded packages can be checked with the command GET DATA using mode 88h (see [13], chapter 3.23). Its response has to show the mandatory Service Package: E1h 0Bh 53h 06h 03h 04h 13h 02h C9h 01h 8Fh 01h 01h
- Identification of the chip (hardware, RMS, crypto library, STS) can be done via GET DATA in mode 8Bh (see [13], chapter 3.23), that must show 76 bytes whereby the bytes contain the following information (first index equals 1):
  byte 1: irrelevant
  byte 2: 78h
  byte 3-5: irrelevant
  byte 6-7: 00h 01h
  byte 8-11: irrelevant
  byte 12-14: 01h 0Bh 02h (02h = Dresden)
  bye 15-n: irrelevant

- The personalisation script files (.csf) can be identified by the version information that can be found as last part of the header information at the beginning of the CSF-file itself. This information is to be compared to the information given in table 1 above (identifier, release version). Example: In case of the TOE 'CardOS V5.0 with Application for QES V1.0', the entry %VERSION% in the csf-file Pre-PersAppSigG.csf version #2 is shown as

```
;>************************************ Version ************************************************;>
;> **** $Id: //Cardos/IsoSec/V5/REL5.0_EVAL/eval/APP/CSF/Pre-PersAppSigG.csf#2 $;>
;>*************************************************************************************************
```

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.SVD_Auth: Authenticity of the SVD
- OE.CGA_QCert: Generation of qualified certificates
- OE.SSCD_Prov_Service: Authentic SSCD provided by SSCD provisioning service
- OE.HI_VAD: Protection of the VAD
- OE.DTBS_Intend: SCA sends data intended to be signed
- OE.DTBS_Protect: SCA protects the data intended to be signed
- OE.Signatory: Security obligation of the signatory
- OE.Attester: Security obligation of the attester for signatures with 4EP
- OE.Env_Admin: Administrator works in trusted environment

- OE.Env_Mass_Signature: Mass signatures are generated in trusted environment only

Details can be found in the Security Target [6], chapter 6.3.

As outlined in the Security Target [6], chapter 2.1 the TOE and its components is delivered after its development phase to the trust center (SSCD provisioning service provider). Therefore, the trust center responsible for initialisation and personalisation has not been part of the evaluation under the ALC assurance class. So the security objective OE.Env_Admin is reflected in appropriate guidance documentation the trust center organisation has to ensure to be fulfilled independently from the personalisation model used (centralized or a decentralized model).

5 Architectural Information

The TOE (CardOS V5.0 with Application for QES, V1.0) 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 [16].

The TOE consists of i) configured software (OS, packages and signature application) ii) the underlying hardware (SLE78CFX*P from Infineon) used to implement the secure signature-creation device (SSCD) and iii) the pertaining guidance documentation.

The operating system (the CardOS V5.0, mask number C901h) is loaded into the ROM (the blocked part of the Flash memory), all packages are loaded in EEPROM (Flash EEPROM) and the application data structure is created by personalization script files.

The external physical interface of the SSCD 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 V5.0 operating system can be found in the “CardOS V5.0 User’s Manual” [13]. Additional information (e.g. modes of operation and application specific command sequences) are given in “User Guidance CardOS V5.0 with Application for QES V1.0” [12], and in the “Administrator Guidance CardOS V5.0 with Application for QES V1.0” [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: Firmware (contains writing routines for non-volatile memory, TRNG tests and sensor checks, reading hardware information, provides a cryptographic library)
- Subsystem 7: ADS (application digital signature)
- Subsystem 8: IC (contains the hardware with all its components)

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 [11] to [15] and 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 Description of test configuration

The configurations that were tested differ in one access right from the TOE that is evaluated. The smart cards and software used for testing were personalised with an access right that allows erasing the EEPROM with the APDU command ERASE FILES. In order to test the TOE as it will be delivered and is intended to be personalised by an administrator, the Evaluation Body devised a test subset with test cards that do not allow erasing the EEPROM. Hence, this configuration is exactly the same as the evaluated one.

For other purposes, where the test stimulation could not be done with means of the external APDU interfaces, an emulator was used.

The Evaluation Body used the same testing equipment as the developer, who provided the test equipment to the Evaluation Body.

7.2 Developer's Test according to ATE_FUN

TOE configurations tested:

The tests were performed with the composite smartcard product CardOS V5.0 with Application for QES, V1.0. All three possible configurations (QES-Germany, QES-Switzerland and QES-Two-PIN-Signatures) were tested appropriately. The different personalisation models (centralized/decentralized) and optional PUK were taken into account. The tests were performed in different life-cycle phases, i.e. in all phases that are in scope after the TOE delivery within the according operational environment.

Testing Approach:

Outgoing from the behaviour defined in the SFRs of the ST, the developer specified test cases for all SFRs in order to cover the TSF. ATE_COV and ATE_DPT were taken into account and mapped to these test cases. The focus of the test cases was the main functionality in the operational state of the TOE, i.e. the creation of signatures and authentication with PIN according to the three configurations.

Additional test cases that could not be performed on a real smartcard (e.g. memory faults and manipulation) were performed in the emulator.

The testing approach has covered all TSFI as described in the functional specification and all subsystems of the TOE design adequately. All configurations as described in the ST are covered. All test results collected in the test reports are as expected and in accordance with the TOE design and the desired TOE functionality.

7.3 Evaluator Tests: Independent Testing according to ATE_IND

Approach for independent testing:

- Examination of developer's testing amount, depth and coverage analysis and of the developer's test goals and plan for identification of gaps.
- Examination whether the TOE in its intended environment, is operating as specified using iterations of developer's tests.
- Independent testing was performed by the evaluator in Essen with the TOE development environment using tests scripts and emulator based on developer test tools.
- TOE test configurations:
- Tests with all three different configurations as described in the ST (QES-Germany, QES-Switzerland, QES-Two-PIN-Signatures)
- Tests were done in different life-cycle phase (before initialization/personalisation and focus on operational usage)

Subset size chosen:

- During sample testing the evaluator chose to sample the developer functional tests using his own test equipment. Emulator tests were repeated but tests with similar test focus were omitted.
- During independent testing the evaluator focussed on the main security functionality as described in the ST, so that all TSF could be covered by at least one test case in order to confirm that the TOE operates as specified.
- Developer tests performed
- The developer performed tests of all TSF and interfaces with script based tests and emulator test cases.
- The evaluator selected a set of functional tests of the developer's testing documentation for sampling. Test cases with similar test focus were omitted.

During the evaluator's TSF subset testing the TOE operated as specified.

7.4 Penetration testing

Overview:

The penetration testing was performed using the test environment of TÜViT. All configurations of the TOE being intended to be covered by the current evaluation were tested.

Penetration testing approach:

Based on a list of potential vulnerabilities applicable to the TOE in its operational environment the evaluators devised the attack scenarios for penetration tests where those potential vulnerabilities could possibly be exploited in the TOE's operational environment.

While doing this, also the aspects of the security architecture described in ADV_ARC were considered for penetration testing. All other evaluation input was used for the creation of the tests as well. Specifically the test documentation provided by the developer was used to find out if there are areas of concern that should be covered by tests of the evaluation body.

The source code reviews of the provided implementation representation accompanied the development of test cases and were used to find test input. The code inspection also supported the testing activity by enabling the evaluator to verify implementation aspects that could hardly be covered by test cases.

In addition the evaluator applied tests and performed code reviews during the evaluation activity of ADV_COMP.1 to verify the implementation of the requirements imposed by the ETR for Composition and the guidance of the underlying platform. This ensured confidence in the security of the TOE as a whole.

The primary focus for devising penetration tests was to cover all potential vulnerabilities identified as applicable in the TOE's operational environment for which an appropriate test set was devised.

TOE test configurations:

The evaluators used TOE samples for testing that were configured according to the ST.

All three configurations as provided by the ST were tested:

- QES-Germany,
- QES-Switzerland,
- QES-Two-PIN-Signatures.

The tests were performed in different test scenarios:

- TOE smart card tested in the TOE development environment at the evaluator's site using developer test tools with automated comparison of expected and actual test results.
- An emulator was used for test cases, which were not possible to perform with a real smart card TOE.
- TOE smart card with dedicated images for the LFI tests at evaluator's site.

The TOE was tested in all life cycle states that are in scope of the usage phase: MANUFACTURING, ADMINISTRATION, OPERATIONAL, DEATH.

As result, no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential High was actually successful in the TOE's operational environment as defined in [6] provided that all measures stipulated by delivery procedures and guidance documentation are applied.

8 Evaluated Configuration

As mentioned above the TOE can be configured according to specific needs on the number of allowed signatures (single signatures; limited (2-255) or unlimited number of signatures in a row; unlimited number of signatures, but secured by two PINs) and in accordance with either QES-Germany, QES-Switzerland, or QES-Two-PIN-Signatures.

Additionally the TOE can be delivered in three different IC sizes.

This certification also covers the following configuration of the TOE: CardOS V5.0 with Application for QES, V1.0. Two personalization models are supported 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 a registration authority (RA), which is locally separated from the certification authority (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 is optional in the DF_QES.
  - The PUK is needed only if unblocking of the PIN shall be possible.
- Centralized model: The certificate(s) are optional in the DF_QES. If the certificate(s) are stored in the DF_QES 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 Attester).
    PIN Set 1 = PIN_1, PUK_1, Transport PIN_1 (Signatory)
    PIN Set 2 = PIN_2, PUK_2, Transport PIN_2 (Attester)
    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 document [9] of the evaluation of the underlying hardware certification [7].
- 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 components AVA_VAN.5 augmented for this TOE evaluation.

The evaluation was not carried out as a re-evaluation.

The evaluation has confirmed:

- PP Conformance: None [9]
- 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

For QES-Germany and QES-Switzerland the following cryptographic algorithms are used by the TOE to enforce its security policy:

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application
Authenticity	RSA-signature generation (RSASSA-PSS and RSASSA-PKCS1-v1_5) using SHA-{256, 384, 512}	PKCS1 v2.1 (RSA), FIPS180-3 (SHA)	moduluslength=1976 - 4096	[17], [20]
	RSA-signature generation (RSASSA-PSS and RSASSA-PKCS1-v1_5)	PKCS1 v2.1 (RSA)	moduluslength=1976 - 4096	[17], [20]

Table 4: TOE cryptographic functionality for QES-Germany and QES-Switzerland

[9] The Protection Profile for Secure signature creation device - Part 2: Device with key generation [21] has been used as a baseline but as the ST includes some additions to the PP, a PP claim "strict" was not possible

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 [17] the algorithms are suitable for authenticity. The validity period as of today of each algorithm is mentioned in the official catalogue [17].

According to [20] the algorithms are suitable for authenticity. An explicit validity period is not given.

For QES-Two-PIN-Signatures the strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But Cryptographic Functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore for this functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context).

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
Authenticity	RSA-signature generation (RSASSA-PSS and RSASSA-PKCS1-v1_5) using SHA-{256, 384, 512}	PKCS1 v2.1 (RSA), FIPS180-3 (SHA)	moduluslength=1976 - 4096	yes
	RSA-signature generation (RSASSA-PSS and RSASSA-PKCS1-v1_5)	PKCS1 v2.1 (RSA)	moduluslength=1976 - 4096	yes

Table 5: TOE cryptographic functionality for QES-Two-PIN-Signatures

10 Obligations and Notes for the Usage of the TOE

The 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 OSPs 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 (trust center, card issuer) and his system risk management process. Future updates of the catalogs [17] and [20] should be considered, too.

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

- The security objectives for the operational environment have to be followed and considered [6, ch. 6.3]
- The software developer (Atos 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 Center for its services, e.g. like a time stamp. The fulfilment of this stipulation is in the responsibility of the Trust Center 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. 4, 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 2019 [17].
- Acording to the User Guidance document [12], chapter 5.12 only specific commands shall be used for the signature application. All other commands shall not be provided for the SCA particularly the command PSO_H, see User Manual [13], chapter 3.34.8, because PSO_H is not in the scope of the TOE. For TOE internally calculated hash values PSO_CDS command has to be used only.

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 Functionality
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 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[10]

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

[6] Security Target BSI-DSZ-CC-0833-2013, Rev. 2.00, Edition 03/2013, 27.03.2013, Security Target 'CardOS V5.0 with Application for QES V1.0', Atos IT Solutions and Services GmbH

[7] Certification Report BSI-DSZ-CC-0758-2012 for Infineon Security Controller M7892 A21 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG
Assurance Continuity Maintenance Report, BSI-DSZ-CC-0758-2012-MA-01, Infineon Security Controller M7892 B11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG

[8] Evaluation Technical Report, CardOS V5.0 with Application for QES V1.0, BSI-DSZ-CC-0833, Version 4, 25.07.2013, TÜViT, (confidential document)

[9] ETR for Composite Evaluation (ETR-COMP), M7892 A21, BSI-DSZ-CC-0758, Version 3, 16.07.2012, TÜViT

[10] Configuration List 'CardOS V5.0 with Application for QES V1.0', Rev. 1.10, Edition 04/2013, Atos IT Solutions and Services GmbH, 08.04.2013 (confidential document)

[11] Administrator Guidance 'CardOS V5.0 with Application for QES V1.0', Rev. 1.30, Edition 03/2013, Atos IT Solutions and Services GmbH, 27.03.2013 (confidential document)

[12] User Guidance 'CardOS V5.0 with Application for QES V1.0', Rev. 1.40, Edition 03/2013, Atos IT Solutions and Services GmbH, 27.03.2013 (confidential document)

[10] specifically

- AIS 25, Version 7, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 8,Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 36, Version 3, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.9, Reuse of evaluation results

[13] CardOS V5.0 User's Manual, Edition 03/2013, Atos IT Solutions and Services GmbH, 03.2013 (confidential document)

[14] CardOS V5.0 Package & Release Notes, Edition 03/2013, Atos IT Solutions and Services GmbH, 03.2013 (confidential document)

[15] Application Digital Signature 'CardOS V5.0 with Application for QES V1.0', Rev. 1.10, Edition 03/2013, Atos IT Solutions and Services GmbH, 27.03.2013 (confidential document)

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

[17] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), Vom 20. Februar 2013, Veröffentlicht am 27. März 2013 im Bundesanzeiger, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

[18] Gesetz über die Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) in der Fassung vom 16. Mai 2001 (BGBl. Jahrgang 2001 Teil I Nr. 22) zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091)

[19] Verordnung zur elektronischen Signatur (Signaturverordnung - SigV) in der Fassung vom 16. November 2001 (BGBl. Jahrgang 2001 Teil I Nr. 59) zuletzt geändert durch die Verordnung vom 15. November 2010 (BGBl. I S. 1542)

[20] Bundesamt für Kommunikation BAKOM, Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur, SR 943.032.1 / Anhang, Ausgabe 4: 8.7.2011

[21] Protection Profiles for Secure signature creation device - Part 2: Device with key generation, prEN 14169-1:2009, BSI-PP0059-2009

[22] PKCS1 v2.1: RSA Cryptographic Standard, RSA Laboratories, Version 2.1, 14.06.2002

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

“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-level design presentation

Assurance Class	Assurance Components
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: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	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	1	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

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0833-2013

Evaluation results regarding development and production environment

The IT product CardOS V5.0 with Application for QES, V1.0 (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 5 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 26 July 2013, 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) Atos IT Solutions and Services GmbH, Otto-Hahn-Ring 6, 81739 Munich, Germany (Software development, Testing, CMS, TOE (i.e. MASK) generation, Documentation)

b) Atos IT Solutions and Services GmbH, Würzburger Str. 121,90766 Fürth, Germany (Software development, Testing, CMS, Documentation)

c) Atos Information Technology GmbH, Lohberg 10, 49716 Meppen, Germany (Documentation)

d) For development and production sites regarding the “M7892 A21 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG“ refer to the certification report BSI-DSZ-CC-0758-2012.

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.