Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0921-2014

for

CardOS V5.3 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-0921-2014

Digital Signature: Secure Signature Creation Device (SSCD)

CardOS V5.3 QES, V1.0

from	Atos IT Solutions and Services GmbH
PP Conformance:	Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation Version 2.01, January 2012, BSI-CC-PP-0059-2009-MA-01
Functionality:	PP conformant 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, 6 August 2014

For the Federal Office for Information Security

Bernd Kowalski
Head of Department

L.S.

SOGIS Recognition Agreement

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 V5.3 QES, V1.0 has undergone the certification procedure at BSI.

The evaluation of the product CardOS V5.3 QES, V1.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 5 August 2014. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and 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 V5.3 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 a composite product referred to as 'CardOS V5.3 QES, V1.0'. It is a smartcard OS with a signature application on the Infineon Security Controller IC M7892 B11 (with three sizes, SLE78CFX2400P with 240kByte flash, SLE78CFX3000P with 300kByte flash and SLE78CFX4000P with 404kByte flash), certified as BSI-DSZ-CC-0782-2012-MA-01.

The TOE allows to generate cryptographically strong signatures based on RSA or ECDSA over previously externally or internally calculated hash values including last round hashing. The TOE generates the signature key pair (SCD/SVD). The TOE is able to protect the secrecy of the internally generated and stored Signature Creation Data (SCD, i.e. secret key) and restricts its usage to the authorized Signatory only. This restriction on usage is done via the well known PIN authentication mechanism.

The customer is a Trust Center which does not configure the TOE completely. It only performs the first configuration step. This Basic Configuration includes the import of symmetric key data individual to the card (depends on ICCSN) used by an Authentication Scheme and generation of the signature key pair. After this step the Application of QES is deactivated since the value of the Transport PIN is not yet imported and thus the Transport Protection cannot be disabled. At this point the card is delivered in a secure way to the end user.

The TOE provides the following functions necessary for devices involved in creating electronic signatures:

1. to generate the signature creation data (SCD) and the corresponding signature verification data (SVD) and
2. to create a single electronic signature
    a) after allowing for the data to be signed (DTBS) to be displayed correctly where the display function is provided by the TOE environment
    b) using appropriate hash functions that are, according to a standard agreed as suitable for electronic signatures
    c) after appropriate authentication of the Signatory by the TOE
    d) after transferring the DTBS, DTBS/R or the intermediate value + remainder of DTBS (last round hashing) by sending the appropriate APDU
    e) using an appropriate cryptographic signature function that employs appropriate cryptographic parameters and key lengths agreed as suitable according to a standard.

The TOE comprises the underlying hardware, the operating system, the SCD/SVD generation, SCD storage and use, hash-generation and signature-creation functionality. An SCIC product containing the TOE may contain additional applications, besides the 'CardOS V5.3 QES, V1.0' (SSCD application), e.g. for electronic identity documents. The SCA and the CGA (and possibly other applications) are part of the immediate environment of the TOE.

The contact based physical interface of the TOE is provided by a connection according to [18]. This interface is used to transmit an APDU command to the TOE and receive the corresponding response APDU from the TOE as specified in [19] and [20].

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation Version 2.01, January 2012, BSI-CC-PP-0059-2009-MA-01 [7].

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 4. 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 Functionality:

TOE Security Functionality	Addressed issue
SF1	User Identification and Authentication
SF2	Access Control provided by the Signature-creation_SFP
SF3	Access Control provided by the SCD/SVD_Generation_SFP
SF4	Access Control provided by the SVD_Transfer_SFP
SF5	Access Control provided by the DF_QES-Configuration_SFP
SF6	Signature Creation
SF7	Protection

Table 1: 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 5.1. 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 4.3.1.

This certification covers the configurations of the TOE as outlined in 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 V5.3 QES, V1.0

The following table outlines the TOE deliverables:

No.	Type	Identifier	Version	Date	Form of Delivery
1	HW	Infineon SLE78CFX*P	M7892 B11	-	IC package
2	SW	CardOS for 240kByte flash	C903	2014-01-15	loaded in protected part of Flash EEPROM
3	SW	CardOS for 300kByte flash	C903	2014-01-15	loaded in protected part of Flash EEPROM
4	SW	CardOS for 404kByte flash	C903	2014-01-15	loaded in protected part of Flash EEPROM
5	SW	EC-library	v.1.02.013	-	loaded in protected part of Flash EEPROM
		SHA-2-library	v.1.01	-	
		RSA-library	v.1.02.013	-	
		Toolbox	v.1.02.013	-	
6	SW	/RsaQesCfg/../ConfigAppRSABase.csf (Configuration script for RSA based QES Base Packet)	2	2014-05-07	electronic file
7	SW	/EcQesCfg/../ConfigAppECBase.csf (Configuration script for EC based QES Base Packet)	3	2014-05-07	electronic file
8	SW	/RsaQesCfg/../ConfigAppADS.csf /EcQesCfg/../ ConfigAppADS.csf (Configuration script for QES ADS Packet, see note 1)	2 3	2014-05-07	electronic file
9	SW	/EcQesCfg/../Defines_EC_secp256r1.csf (Constants definitions for EC key pair with secp256r1)	3	2014-05-07	electronic file
10	SW	/EcQesCfg/../Defines_EC_secp384r1.csf (Constants definitions for EC key pair with secp384r1)	3	2014-05-07	electronic file
11	SW	/EcQesCfg/../Defines_EC_brainpoolP256r1.csf (Constants definitions for EC key pair with brainpoolP256r1)	3	2014-05-07	electronic file
12	SW	/EcQesCfg/../Defines_EC_brainpoolP384r1.csf (Constants definitions for EC key pair with brainpoolP384r1)	3	2014-05-07	electronic file

No.	Type	Identifier	Version	Date	Form of Delivery
13	SW	/RsaQesCfg/../Defines_RSA_2048.csf (Constants definitions for RSA key pair, length 2048 bits)	2	2014-05-07	electronic file
14	SW	/RsaQesCfg/../Defines_RSA_2560.csf (Constants definitions for RSA key pair, length 2560 bits)	2	2014-05-07	electronic file
15	SW	/RsaQesCfg/../Defines_RSA_3072.csf (Constants definitions for RSA key pair, length 3072 bits)	2	2014-05-07	electronic file
16	SW	/RsaQesCfg/../Defines_RSA_3584.csf (Constants definitions for RSA key pair, length 3584 bits)	2	2014-05-07	electronic file
17	SW	/RsaQesCfg/../Defines_RSA_4096.csf (Constants definitions for RSA key pair, length 4096 bits)	2	2014-05-07	electronic file
18	DOC	CardOS V5.3, User’s Manual [13]	05/2014	2014-05	PDF file
19	DOC	Packages & Release Notes 'CardOS V5.3 QES, V1.0' [14]	05/2014	2014-05	PDF file
20	DOC	Administrator Guidance 'CardOS V5.3 QES, V1.0' [15]	R1.20	2014-05-07	PDF file
21	DOC	User Guidance 'CardOS V5.3 QES, V1.0' [16]	R1.30	2014-05-02	PDF file
22	DOC	Application Digital Signature 'CardOS V5.3 QES, V1.0' [17]	R1.10	2014-05-07	PDF file

Table 2: Deliverables of the TOE

Note 1: Please note that depending on EC or RSA for ConfigAppADS.csf the correct directory must be used.

2.1 TOE delivery process

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.

Components #1 to #5 are actually delivered as one item (IC platform containing the software mask) to the customer trust center (TC) or to entities on behalf of the TC. The components from number #6 to #17 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. Items #6 and #7 contain the Basic Configuration for Application for QES (RSA or EC based signature creation). Item #8 contains the ADS Configuration to finalize the configuration provided by items #6 or #7. The Trust Center is allowed to make changes or extensions in items #6, #7 and #8 which are marked by the developer.

These changes or extensions concern:

- in case of EC which domain parameters of an EC shall be imported,
- in case of RSA which bit length shall be used,
- whether a PUK shall be available or not or
- which value shall be used for the retry counter of the Signatory PIN

When the TOE is leaving the TC the Application for QES is deactivated since the Transport PIN is not imported by the TC during the Basic Configuration. In this state the TOE however provides an Authentication Scheme for setting up a secure mutually authenticated Trusted Channel for securing all data from modification and disclosure and providing the (local) RA a mechanism to authenticate itself to the TOE and vice versa the TOE to the (local) RA.

To perform the ADS Configuration the TOE provides the following functions which are performed securely using the means of a mutually authenticated Trusted Channel:

1. Export of the public key data of the generated key pair.
2. Optional creation including update of EFs / DFs below DF_QES, e.g. with the qualified certificate and the certificate of the Certification Authority which generates the qualified certificate. The RA is able to remove EFs, DFs below DF_QES, too.
3. Import of the Transport PIN, from now on the Application for QES is prepared for activation by the Signatory.

The ADS Configuration can be done at a (local) RA or at a (remote) RA using the Internet.

This chapter makes the following presumptions:

1. Standard commercial practices apply, i.e.
   - the Trust Center in its role as customer initializes the delivery of (parts of) the TOE by placing an order and does not accept (parts of) TOE deliveries they had not placed an order for beforehand and
   - the customer is free to choose the delivery address according to his organization (e.g. to have the ordered modules directly sent to his local embedder).
2. Definition of appropriate procedures to preserve confidentiality, integrity and authenticity of the TOE parts (details on which property to preserve for which TOE part are given in a TOE's Administrator Guidance documentation) is the responsibility of the Trust Center. Therefore the figure only depicts which property has to be preserved for which item.
3. The technical and organizational procedures that are defined to preserve the integrity and authenticity of the completed hardware allow applying standard commercial practice for packaging, storage and distribution and thus do not require describing concrete delivery chains, i.e. whether the hardware, that is delivered by the TOE developer is sent directly from the chip manufacturer to the Trust Center or takes a detour through the stock of the TOE developer and some distributors is irrelevant.
4. The Trust Center is free to organize and define its processes to its liking, provided its security policy implements the requirements defined in the TOE's Administrator Guidance.

2.2 Identification of the TOE by the end user

To verify that the user has the correct card, it can be identified by any entity with the command “GET DATA” using specific modes (see [15] chap. 5.3.1, [16] chap. 4.1, [17] chap. 4.1.1 and [13] chap. 3.24):

- Mode 80h must return the product name, version and copyright string "CardOS V5.3, 2014" ("43h 61h 72h 64h 4fh 53h 20h 56h 35h 2eh 33h 2ch 20h 32h 30h 31h 34h 00h").
- Mode 82h returns the OS version "C903" for CardOS V5.3.
- Identification of the chip (HW, RMS, crypto library, STS) can be done via “Get Data” in mode 8Bh (see [13] chap. 3.24), that for the SLE78CFX*P (M7892 B11) manufactured in Dresden must match the following pattern:

Index	1	2	...	6	7	...	12	13	14
Value	...	78h	...	00h	01h	...	01h	0Bh	02h

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)

byte 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. In case of the TOE 'CardOS V5.3 QES, V1.0', the entry %VERSION% (see below) has to show the same information as given in the certification report.

```
;> **** ********************************** Version ***********************************
;> ****
;> **** $Id:
//Cardos/IsoSec/V5/REL5.3/eval/APP/CSF/RsaQesCfg/Delivery_version/ConfigAppADS.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:

1. OE.SVD_Auth (Authenticity of the SVD)
2. OE.CGA_QCert (Generation of qualified certificates)
3. OE.SSCD_Prov_Service (Authentic SSCD provided by SSCD provisioning service)
4. OE.HID_VAD (Protection of the VAD)
5. OE.DTBS_Intend (SCA sends data intended to be signed)
6. OE.DTBS_Protect (SCA protects the data intended to be signed)
7. OE.Signatory (Security obligation of the signatory)
8. OE.Env_Admin (Administrator works in trusted environment)
9. OE.Env_RA (RA as a trusted environment)

The administrative functions of "Administrator" users are performed within a trusted environment. Details can be found in the Security Target [6], chapter 6.3.

As outlined in the Security Target [6], chapter 3.4.1 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.

5 Architectural Information

The TOE design presents a more detailed modularisation of the TOE and its subsystems. The TOE can be divided into the following eight subsystems and the underlying hardware:

S1 - Protocol Manager (monitors the correct data transfer),

S2 - Command Manager (implements the command identification),

S3 - Command Layer (contains the interpretation of all CardOS commands),

S4 - Service Layer (contains service and security routines),

S5 - System Layer (contains system and basic routines),

S6 - Firmware (contains writing routines for non-volatile memory, RNG tests and sensor checks, reading hardware information, provides a cryptographic library)

S7 - ADS (application digital signature),

S8 - IC (contains the hardware with all its components).

The general functionality and the sequence of operations processed in the TOE can be structured as follows:

1. after connecting the voltage, the clock and reset signal, the operation begins with S1 sending an ATR (answer to reset) to the IFD (via CPU).
2. S1 receives a command from the IFD (via CPU).
3. S2 identifies the command, submitted by S1.
4. S3 interprets and checks the command to be executed.
5. S4 sets the respective access right (data access denied or permitted) if applicable.
6. S1 sends the execution status (return code, and if applicable user data) to the respective IFD (via CPU)
7. the TOE proceeds with step (2) or the loop is broken by taking the card out of the reader.

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 Exact Description of the 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 V5.3 QES, V1.0 on the IC Infineon M7892 B11. From the three different memory sizes of the IC (SLE78CFX2400P, SLE78CFX3000P or SLE78CFX4000P, all design step B11) only the SLE78CFX3000P platform has been tested by the developer.

Configurable options beside the main option SCD/SVD Key Algorithm (EC or RSA) are:

- Anchor Key Algorithm (key algorithm of the anchor key used for secure messaging, 3DES or AES),
- K_Appl_QES Key Algorithm (key algorithm used for secure messaging, 3DES or AES),
- PUK (whether a PUK will be used or not) and
- PIN retry counter value (indicates whether the retry counter will be fixed or variable).

The combination of these options is not exhaustive and complete with respect to all possible combinations. The developer tested the following configurations:

1. EcQesCfg_ellipticCurve:
    - four different key lengths: brainpoolP256r1, brainpoolP384r1, secp256r1, secp384r1 with fixed combination of
    - Anchor Key Algorithm 3DES,
    - K_Appl_QES Key Algorithm 3DES,
    - Without PUK and
    - PIN retry counter value fixed=10
2. RsaQesCfg_keyLen:
    - five different key lengths: 2048, 2560, 3072, 3584 and 4096 bits with fixed combination of
    - Anchor Key Algorithm AES,
    - K_Appl_QES Key Algorithm AES,
    - With PUK and
    - PIN retry counter value variable (min=floor((min pinlen)/2))

Both main configurations (EcQesCfg_ellipticCurve and RsaQesCfg_keyLen) were tested appropriately. The differences (e.g. PIN retry counter fixed/variable 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:

Originating 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 two configurations.

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

Verdict for the activity:

The testing approach covers all TSFI as described in the functional specification and all subsystems of the TOE design adequately. All main configurations as described in the Security Target 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 test scripts and emulator based on developer test tools.

TOE test configurations:

- Tests with all three different configurations as described in the Security Target:
  - The signature-creation function uses the ECDSA or the RSA algorithm for creating signatures
  - A PUK for unblocking the PIN is available or not
  - The retry counter of the PIN depends on the length of the PIN or not.
- Tests were done in different life-cycle phases (before initialization/personalisation and focus on operational usage) and with different platform chip sizes (SLE78CFX2400P, SLE78CFX3000P and SLE78CFX4000P)

Subset size chosen:

- During sample testing the evaluator chose to sample the developer functional tests at the Evaluation Body for IT Security in Essen. Emulator tests with similar test focus were omitted.
- During independent testing the evaluator focussed on the main security functionality as described in the Security Target [6], with 35 evaluator test cases so that all TSF could be covered by at least one test case in order to confirm that the TOE operates as specified.

Security functions tested:

- User Identification and Authentication
- Access Control provided by the Signature-creation_SFP
- Access Control provided by the SCD/SVD_Generation_SFP
- Access Control provided by the SVD_Transfer_SFP

- Access Control provided by the DF_QES-Configuration_SFP
- Signature Creation
- Protection

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.

Verdict for the activity:

- During the evaluator's TSF subset testing the TOE operated as specified.
- The evaluator verified the developer's test results by executing a sample of the developer's tests and verifying the test results for successful execution.

7.4 Penetration testing according to AVA_VAN

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 created within the work unit AVA_VAN.5-5 the evaluators devised the attack scenarios for penetration tests when they were of the opinion, that those potential vulnerabilities could 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 Security Target [6]. The samples were identified by the evaluator using the method as described in the guidance documentation [15], [16], [17]

- Tests with all three different configurations as described in the Security Target:

  - The signature-creation function uses the ECDSA or the RSA algorithm for creating signatures
  - A PUK for unblocking the PIN is available or not
  - The retry counter of the PIN depends on the length of the PIN or not.
- Tests were done in different life-cycle phases (before initialization/personalisation and focus on operational usage) and with platform chip configuration identified by SLE78CFX3000P.

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. The automated tests also covering the repetition of developer's test have been performed with different platform chip sizes (SLE78CFX2400P, SLE78CFX3000P and SLE78CFX4000P).
- 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 on SLE78CFX3000P for the LFI and Leakage tests at evaluator's site.

The TOE was tested in all life cycle states that are in scope of the usage phase (see [6], chap. 3.4):

- MANUFACTURING
- ADMINISTRATION
- OPERATIONAL
- DEATH

Verdict for the sub-activity:

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential High was actually successful in the TOE's operational environment as defined in the Security Target [6] provided that all measures required by the developer are applied.

8 Evaluated Configuration

The TOE CardOS V5.3 QES V1.0 on the IC SLE78CFX*P (M7892 B11) is certified in all of its three HW configurations as described in the Security Target [6]. The TOE can be delivered in three different IC sizes: On IC SLE78CFX2400P (240 kByte flash), SLE78CFX3000P (300 kByte flash) or SLE78CFX4000P (404kByte flash), that are all certified under the same certification ID for the M7892 B11 (BSI-DSZ-CC-0782-2012-MA-01). Thus, the IC size does not have an impact on the TSF of the TOE.

Related to functionality there are different configurations (see [6], chap. 8.2.3) as follows:

1. A configuration of the TOE shall use only one of the following SFRs:
   a) FIA_AFL.1/VarLenPINRC
   b) FIA_AFL.1/FixedLenPINRC

2. A configuration of the TOE shall use only one of the following groups of SFRs:
   a) FCS_CKM.1/RSA, FCS_COP.1/RSA
   b) FCS_CKM.1/EC, FCS_COP.1/EC
3. Depending on which SFR of (2) shall be used the domain parameters of an EC have to be imported or not. This concerns the following SFRs:
   a) FMT_SMF.1
   b) FMT_MTD.1/Ini-Data
4. Only if a configuration needs a PUK, the TOE shall use SFR
   a) FIA_AFL.1/PUK
5. If a configuration does not need a PUK, the RAD of the Signatory consists only of a PIN. If a configuration needs a PUK, the RAD of the Signatory consists of PIN and PUK. This concerns the following SFRs:
   a) FIA_UID.1
   b) FIA_UAU.1
   c) FMT_SMF.1
   d) FMT_MTD.1/RAD
   e) FMT_MTD.1/Signatory

The SFRs listed above at c) and e) are used by all configurations, just the scope of this SFR is a little bit different. E.g. FMT_MTD.1/Ini-Data deals either with initialisation data which includes domain parameters or is not depending on the algorithm chosen.

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 EAL4 (AIS 34) and guidance specific for the technology of the product [4].

The following guidance specific for the technology was used:

(i) The Application of CC to Integrated Circuits

(ii) The Application of Attack Potential to Smartcards

(iii) Composite product evaluation for Smart Cards and similar devices. According to this concept the relevant guidance documents of the underlying platform and the documents ETR for Composition from the platform evaluations (i.e. on hardware [9], [10] have been applied in the TOE evaluation.

(see [4], AIS 25, AIS 26, AIS 32, AIS 36)

For RNG assessment the scheme interpretations AIS 20 / AIS 31 were used (see [4]).

A document ETR for composite evaluation according to AIS 36 has not been provided in the course of this certification procedure. It could be provided by the ITSEF and submitted to the certification body for approval subsequently.

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

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 has confirmed:

- PP Conformance: Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation Version 2.01, January 2012, BSI-CC-PP-0059-2009-MA-01 [7]
- for the Functionality: PP conformant
  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. The TOE uses the certified cryptographic libraries of the underlying certified IC M7892 B11 (BSI-DSZ-CC-0782-2012-MA-01). The following table lists the cryptographic algorithms as used in a specific field of operation:

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application[1]	Validity Period
Authenticity	Elliptic Curve Digital Signature Generation Algorithm (ECDSA- Signature generation)	ANSI X9.62 - 2005 section 7.3 [32] and ISO/IEC 15946-2:2002 6.2.2. + 6.2.3 [33] and NIST-FIPS-PUB-186-4, D.2.3 [27] "Curve P-256", NIST-FIPS-PUB-186-4, D.2.4 "Curve P-384" [27], „brainpoolP256r1“, „brainpoolP384r1“, [35] 3.4 + 3.6	256 and 384	[21], [22][2]	Until end of 2020

Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application[1]	Validity Period
Authenticity	Elliptic Curve Digital Signature Generation Algorithm (ECDSA- Signature generation) using last round of SHA-{256, 384, 512}	ANSI X9.62 – 2005 [32] section 7.3 and ISO/IEC 15946-2:2002 [33] 6.2.2. + 6.2.3 and NIST-FIPS-PUB-186-4 [27] D.2.3 "Curve P-256", D.2.4 "Curve P-384", NIST-FIPS-PUB-180-4 [26] chapters 6.2, 6.4, 6.5, „brainpoolP256r1“, „brainpoolP384r1“, [35] 3.4 + 3.6	256 and 384	[21], [22][2]	Until end of 2020
Authenticity	Elliptic Curve Digital Signature Generation Algorithm (ECDSA- Signature generation) using SHA-{256, 384, 512}	ANSI X9.62 – 2005 [32] section 7.3 and ISO/IEC 15946-2:2002 [33] 6.2.2. + 6.2.3 and NIST-FIPS-PUB-186-4 [27] D.2.3 "Curve P-256", D.2.4 "Curve P-384", „brainpoolP256r1“, „brainpoolP384r1“, [35] 3.4 + 3.6 and; NIST-FIPS-PUB-180-4 [26] chapters 6.2, 6.4, 6.5	256 and 384	[21], [22][2]	Until end of 2020
Authenticity	Rivest-Shamir-Adleman (RSA) Signature Generation	PKCS1 v2.1 RFC3447 [34], section 5.2.1 RSASP1	2048 - 4096	[21], [22][2]	Until end of 2020
Authenticity	Rivest-Shamir-Adleman (RSA) Signature Generation using last round of SHA-{256, 384, 512}	PKCS1 v2.1 RFC3447 [34], section 5.2.1 RSASP1; NIST-FIPS-PUB- 180-4 [26] chapters 6.2, 6.4, 6.5	2048 - 4096	[21], [22][2]	Until end of 2020
Authenticity	Rivest-Shamir-Adleman (RSA) Signature Generation using SHA-{256, 384, 512}	PKCS1 v2.1 RFC3447 [33], section 5.2.1 RSASP1; NIST-FIPS-PUB-180-4 [26] chapters 6.2, 6.4, 6.5	2048 - 4096	[21], [22][2]	Until end of 2020

Table 3: TOE cryptographic functionality in a specific field of operation

Notes for Table 3:

[1] The “Standard of Application” is:

- in case of configurations applying for an Austrian Confirmation (SigG/SigV) [22] chapter “Anhang”
- in case of configurations applying for a German Confirmation (SigG/SigV) [21]

[2] No explicit information on validity periods is provided by [22]

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 these 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).

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
1	Authenticated Key Agreement	Symmetric Authentication Scheme with key agreement	CWA-14890-1, chapter 8.8 improved by SHA-256 [25]		
		using TDES	see No. 3	168	No
		and Retail-MAC	see No. 5		
		and SHA-256	see No. 2		
		and Challenge		64	
		or using AES	see No. 4	128	No
		and CMAC	see No. 6		
		and SHA-256	see No. 2		
		and Challenge		64	
2	Cryptographic Primitive (see note 1)	SHA-{256, 384, 512}	NIST-FIPS-PUB-180-4 [26] chap. 6.2, 6.4, 6.5	none	Yes
3	Confidentiality	TDES	NIST Special Publication 800-67 Version 1.1 [30]	168	Yes
	(see note 2)	in CBC mode	NIST-800-38A-2001 [29]		
4	Confidentiality (see note 3)	AES	FIPS PUB 197 [28]	128, 192 and 256	Yes
		in CBC mode	NIST-800-38A-2001 [29]		
5	Integrity	TDES	NIST, NIST Special Publication 800-67 Version 1.1 [30]	168	No
	(see note 2)	and Retail-MAC	ISO-IEC-9797-1-2011 [31]		
6	Integrity (see note 3)	AES	FIPS PUB 197 [28]	128, 192 and 256	Yes
		and CMAC	ISO-IEC-9797-1-2011 [31]		

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
7	Authenticity (see note 4)	RSA signature generation	PKCS1 v2.1 RFC3447 [34], section 5.2.1 RSASP1	modulus lenght= 2048 - 4096	Yes
		padding with RSASSA-PSS and RSASSA-PKCS1-v1_5			
		using SHA-{256, 384, 512}	see No. 2		
8	Authenticity (see note 5)	ECDSA	ANSI X9.62 – 2005 [32] section 7.3 and ISO/IEC 15946-2:2002 [33] 6.2.2. + 6.2.3		Yes
		using curve "curve P-256" with SHA-256	NIST-FIPS-PUB-186-4 D.2.3 "Curve P-256" [27]	256	
		using curve "curve P-384" with SHA-384	NIST-FIPS-PUB-186-4 D.2.4 "Curve P-384" [27]	384	
		using brainpoolP256r1 with SHA-256	RFC-5639-2010-03 [35] chapter 3.4	256	
		using brainpoolP384r1 with SHA-384	RFC-5639-2010-03 [35] chapter 3.6	384	

Table 4: TOE cryptographic mechanisms used

Notes for Table 4:

1. This TOE uses the SHA-2 crypto library v1.01 of the underlying chip SLE78CFX*P (M7892 B11). For the hash algorithms SHA-256 and SHA-512 see [36], 7.1.4.10 SHA-2 Operation. A SHA-384 value is computed by CardOS V5.3 from a SHA-512 value according to [26], chapter 6.5.
2. This TOE uses TDES provided by the underlying chip SLE78CFX*P (M7892 B11). For TDES operation see [36], chapter 7.1.4.2 Triple-DES Operation.
3. This TOE uses the AES provided by the underlying chip SLE78CFX*P (M7892 B11). For AES operation see [36], chapter 7.1.4.3 AES Operation.
4. This TOE uses the RSA crypto library v1.02.013 of the underlying chip SLE78CFX*P (M7892 B11). For the signature generation see [36], chapter 7.1.4.4 Rivest-Shamir-Adleman (RSA) operation.
5. This TOE uses the EC crypto library v1.02.013 of the underlying chip SLE78CFX*P (M7892 B11). For the "Elliptic Curve Digital Signature Algorithm (ECDSA)" see [36], chapter 7.1.4.7 Elliptic Curve DSA (ECDSA) operation.

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 [21] the algorithms are suitable for authenticity. The validity period of each algorithm is mentioned in the official catalogue [21].

According to [22] the algorithms are suitable for authenticity. An explicit validity period is not given.

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 of 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 catalog [21] 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 (see [6], chap. 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.
- Besides the general recommendations concerning the quality of a PIN/PUK (e.g. length, retry count, etc.) as stated in the User Guidance [16], sec. 4, the user must be urged to choose a non trivial PIN/PUK before using the TOE in its operational state.
- When configuring the QES application for EC or RSA the configuration script for QES (ConfigAppADS.csf) in the respective directory (EcQesCfg or RsaQesCfg) shall be used.

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
DF	Dedicated File
DTBS/R	Data to be signed/Representation
EAL	Evaluation Assurance Level
EC/ECC	Elliptic Curve/Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EF	Elementary File
ETR	Evaluation Technical Report
HW	Hardware
ICCSN	Integrated Circuit Card Serial Number
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
PIN	Personal Identification Number
PP	Protection Profile
PUK	Personal Unblocking Key
QES	Qualified Electronic Signature (qualifizierte elektronische Signatur)
RA	Registration Authority
RAD	Reference Authentication Data
RMS	Resource Management System
RSA	Rivest-Shamir-Adleman Algorithm
SAR	Security Assurance Requirement
SCA	Signature Creation Application
SCIC	Smart Card IC
SFP	Security Function Policy
SFR	Security Functional Requirement
SigG	Signaturgesetz
SigV	Signatureverordnung
SSCD	Secure Signature Creation Device

ST	Security Target
STS	Self Test Software
SVD	Signature Verification Data
SW	Software
TC	Trust Center
TDES/3DES	Triple Data Encryption Standard (using 3 keys)
TOE	Target of Evaluation
TSF	TOE Security Functionality
VAD	Verfication 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 - A 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 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012

[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 in the BSI Website

[6] Security Target BSI-DSZ-CC-0921-2014, Version 1.61, 23 July 2014, Security Target 'CardOS V5.3 QES, V1.0', Atos IT Solutions and Services GmbH, (public document)

[7] Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation Version 2.01, January 2012, BSI-CC-PP-0059-2009-MA-01, 23 January 2012, CEN / CENELEC (TC224/WG17)

[8] Evaluation Technical Report BSI-DSZ-CC-0921-2014, Version 3.0, 31 July 2014, TÜV Informationstechnik GmbH, (confidential document)

[9] Certification Report BSI-DSZ-CC-0782-2012 for 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, 11 September 2012, Bundesamt für Sicherheit in der Informationstechnik, (public document)

[10] Assurance Continuity Maintenance Report BSI-DSZ-CC-0782-2012-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, 05 September 2013, Bundesamt für Sicherheit in der Informationstechnik, (public document)

---

[8] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 8, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 9, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- 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 4, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2, Reuse of evaluation results

[11] ETR for Composite Evaluation (ETR-COMP), M7892 B11, BSI-DSZ-CC-0782, Version 5, 20 March 2014, TÜV Informationstechnik GmbH, (confidential document)

[12] Configuration List 'CardOS V5.3 QES, V1.0', Revision 1.30, 30 July 2014, Atos IT Solutions and Services GmbH, (confidential document)

[13] Users Manual CardOS V5.3, Edition 05/2014, Atos IT Solutions and Services GmbH, (confidential document)

[14] Packages & Release Notes 'CardOS V5.3 QES, V1.0', Edition 05/2014, Atos IT Solutions and Services GmbH, (confidential document)

[15] Administrator Guidance 'CardOS V5.3 QES, V1.0', Revision 1.20, 07 May 2014, Atos IT Solutions and Services GmbH, (confidential document)

[16] User Guidance 'CardOS V5.3 QES, V1.0', Revision 1.30, 02 May 2014, Atos IT Solutions and Services GmbH, (confidential document)

[17] Application Digital Signature 'CardOS V5.3 QES, V1.0', Revision 1.10, 07 May 2014, Atos IT Solutions and Services GmbH, (confidential document)

[18] ISO 7816 Part 3: Electronic Signals and Transmission Protocols – ISO/IEC 7816-3:1997/Amd 1:2002

[19] ISO 7816 Part 4: Interindustry Commands for Interchange – ISO/IEC 7816-4:1995/Amd 1:1997

[20] ISO 7816-8; Identification cards – Integrated circuit cards – Part 8: Commands for security operations, 2004

[21] Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Absatz 1 bis 3 SigG vom 16. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nummer 2 SigV vom 16. November 2001, Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 21. Januar 2014, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen

[22] Gesamte Rechtsvorschrift für Signaturverordnung 2008, Fassung vom 25.07.2013, Langtitel: “Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 - SigV 2008, BGBl. II Nr. 3/2008 vom 7. Jänner 2008) in der Fassung BGBl. II Nr. 401/2010 vom 9. Dezember 2010.”, www.ris.bka.gv.at, Bundeskanzleramt Österreich

[23] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG) Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), das durch Artikel 4 Absatz 111 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist

[24] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV) Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), die durch Artikel 4 Absatz 112 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist

[25] CWA 14890-1, March 2004, Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic requirements

[26] Secure Hash Standard (SHS), Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, MD 20899-8900, March 2012

[27] Digital Signature Standard (DSS), Information Technology Laboratory, National Institute of Standards and Technology Gaithersburg, MD 20899-8900, July 2013

[28] Federal Information Processing Standards Publication 197, National Institute of Standards and Technology Gaithersburg, MD 20899-8900, 26 November 2001, Announcing the Advanced Encryption Standard (AES)

[29] Recommendation for Block Cipher Modes of Operation, National Institute of Standards and Technology Gaithersburg, MD 20899-8900, December 2001

[30] NIST Special Publication 800-67, Version 1.1, National Institute of Standards and Technology Gaithersburg, MD 20899-8900, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Revised 19 May 2008

[31] ISO-IEC-9797-1-2011, ISO/IEC, Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, 2001-03

[32] ANS X9.62-2005 Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA), Date Approved: 16 November 2005, American National Standard for Financial Services

[33] ISO/IEC 15946-2, Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signatures, First edition 2002-12-01

[34] Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, February 2003

[35] RFC 5639, Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010

[36] Maintenance Security Target Lite M7892 B11, Version 1.4, 26 August 2013, Infineon Technologies AG, (public document)

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-0921-2014

Evaluation results regarding development and production environment

The IT product CardOS V5.3 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 6 August 2014, 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:

No.	Site	Task within the evaluation
a)	Atos IT Solutions and Services GmbH, Otto-Hahn-Ring 6, 81739 Munich	Software development, Testing, CMS, TOE (i.e. MASK) generation, Documentation
b)	Atos IT Solutions and Services GmbH, Wuerzburger Str. 121, 90766 Fuerth	Development site
c)	Atos Information Technology GmbH, Lohberg 10, 49716 Meppen	Development site (creation of evaluation documentation only)
d)	Atos IT Solutions and Services d.o.o., Zrinsko-Frankopanska 64, 21000 Split/Croatia	Development and testing of the TOE

For development and production sites regarding the 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 refer to the certification report of BSI-DSZ-CC-0782-2012 [9] part D, Annex B.

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.