Certification Report

BSI-DSZ-CC-0967-2016

for

CardOS DI V5.3 EAC/PACE Version 1.0

from

Atos IT Solutions and Services GmbH

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0967-2016 (*)

Security IC with MRTD EAC/PACE Application

CardOS DI V5.3 EAC/PACE Version 1.0

from	Atos IT Solutions and Services GmbH
PP Conformance:	Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE, Version 1.3.2, 5 December 2012, BSI-CC-PP-0056-V2-2012-MA-02
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_DVS.2, ATE_DPT.2, AVA_VAN.5

SOGIS
Recognition Agreement

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 Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) 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 and Notification. For details on the validity see Certification Report part A chapter 4

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.

Common Criteria
Recognition Arrangement
for components up to
EAL 2

Bonn, 23 June 2016

For the Federal Office for Information Security

Bernd Kowalski   L.S.
Head of Department

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

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:

- Act on the Federal Office for Information Security[2]

- BSI Certification and Approval Ordinance[3]

- BSI Schedule of Costs[4]

- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)

- DIN EN ISO/IEC 17065 standard

- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]

- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]

- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1] also published as ISO/IEC 15408.

- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045.

- 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 SOGIS Technical Domains only.

---

[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 Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

[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

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

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. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogisportal.eu.

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

This certificate is recognized under SOGIS-MRA for all assurance components selected.

2.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

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 certificate is recognized according to the rules of CCRA-2014, i.e. up to and including CC part 3 EAL 2 components. The evaluation contained the components ADV_FSP.4, ADV_IMP.1, ADV_TDS.3, ALC_CMC.4, ALC_CMS.4, ATE_COV.2, ATE_DPT.2 and AVA_VAN.5 that are not mutually recognised in accordance with the provisions of the CCRA-2014, for mutual recognition the EAL 2 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 DI V5.3 EAC/PACE Version 1.0 has undergone the certification procedure at BSI.

The evaluation of the product CardOS DI V5.3 EAC/PACE Version 1.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 21 June 2016. 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

- 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 or in the CC itself.

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 order to avoid an indefinite usage of the certificate when evolved attack methods require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 23 June 2016 is valid until 22 June 2021. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security

---

6   Information Technology Security Evaluation Facility

Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,

3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

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 DI V5.3 EAC/PACE Version 1.0 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

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 DI V5.3 EAC/PACE Version 1.0 provided by Atos IT Solutions and Services GmbH and based on the hardware platform M7892 B11 by Infineon. It is an electronic travel document (Machine Readable Travel Document – MRTD) representing a contactless/contact-based smart card programmed according to ICAO Technical Report "Supplemental Access Control" [17] and additionally providing the Extended Access Control according to the ICAO documents [18] and [19] and the Technical Guideline TR-03110, Version 2.10 [20], respectively. The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to the Protection Profile [8]. Additionally, Active Authentication according to the ICAO Technical Report [21] is provided.

The Security Target [6] is the basis for this certification. It is based on the following certified Protection Profile:

● Machine Readable Travel Document with "ICAO Application" Extended Access Control with PACE, Version 1.3.2, 5 December 2012, BSI-CC-PP-0056-V2-2012-MA-02 [8].

The Protection Profile above is strict conformant to the following Protection Profile. In result, the TOE is also conformant to this PP.

● Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), Version 1.0, 2 November 2011, BSI-CC-PP-0068-V2-2011 [9].

Please note that in consistency to the claimed protection profile BSI-CC-PP-0056-V2-2012-MA-02 the security mechanisms *Password Authenticated Connection Establishment* and *Extended Access Control* are in the focus of this evaluation process. The further security mechanism *Basic Access Control* is subject of the separate evaluation process BSI-DSZ-CC-0968-2016.

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 ALC_DVS.2, ATE_DPT.2, AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 8.1. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functionality	Addressed Issue
User Identification and Authentication	Provides mechanisms for identification and authentication of the user roles.
Advanced Inspection Procedure with PACE	Provides Advanced Inspection Procedure.
Protocols such as PACE, Chip Authentication, Active Authentication, Terminal Authentication	Provides authentication protocols PACE, Chip Authentication, Active Authentication, and Terminal Authentication.
Passive Authentication	Supports Passive Authentication.

TOE Security Functionality	Addressed Issue
Read access at phase OPERATIONAL	Regulates read access at phase OPERATIONAL to the Logical Travel Document and the Document Security Object.
Write access at phase OPERATIONAL	Regulates write access at phase OPERATIONAL.
Establishing the trusted channel	Provides a communication channel between the TOE and the terminal, permits the terminal to initiate communication via the trusted channel and enforces communication via the trusted channel for any data exchange between the TOE and the terminal.
Test features	Regulates test features of the TOE which are disabled before the card leaves the IC manufacturer's site.
Protection of the TSF, TSF data and user data	Provides protection of the TSF, TSF data and user data against fraudulent attacks.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] chapter 9.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 5.1.1. 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 5.2, 5.3, and 5.4.

This certification covers the following configurations of the TOE (for details refer to chapter 8 of this report):

● the circuitry of the MRTD's chip (the integrated circuit, IC),

● the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,

● the antenna,

● the IC Embedded Software (operating system),

● the ePassport Application, and

● the associated guidance documentation.

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 DI V5.3 EAC/PACE Version 1.0

The following table outlines the TOE deliverables:

No.	Type	Item / Identifier	Version	Form of Delivery
1	Hardware (chip)	SLE78CLFX*P (M7892 B11)	M7892 B11	Chip or module
2		Antenna	-	Inlay
3	Software	CardOS DI V5.3 for 300kB	C902	Loaded in protected part of flash EEPROM
4		CardOS DI V5.3 for 404kB	C902	
5		EC library	1.02.013	
		RSA library	1.02.013	
		Toolbox	1.02.013	
		SHA-2 library	v1.01	
6	ICAO Package L	V53DI_ICAO_ext_Package_L.csf	8	*[8]
7	ICAO Package P	V53DI_ICAO_ext_Package_P.csf	8	*[8]
8	Initialization script for EC based ePassport L(ogical)	ECC/ConfigApp_Init_L.csf	7	*[8]
9	Initialization script for EC based ePassport P(hysical)	ECC/ConfigApp_Init_P.csf	7	*[8]
10	Pre-Personalization script for EC ePassport L	ECC/ConfigApp_Pre.csf	8	*[8]
11	Personalization script for EC ePassport L	ECC/ConfigApp_Person.csf	7	file
12	Constant data for EC based ePassport	ECC/ConstantData.csf	6	*[8]
13	Configuration data for EC based Pre-Personalization	ECC/ConfigData_Pre.csf	7	*[8]
14	Configuration data for EC based Personalization	ECC/ConfigData_Person.csf	8	file

---

[8] Not the script files themselves are delivered to the personalization agent but the initialized and pre-personalised inlay created by using these files. For more information, see the following paragraph.

No.	Type	Item / Identifier	Version	Form of Delivery
15	Initialization script for RSA based ePassport L	RSA/ConfigApp_Init_L.csf	7	[8]
16	Initialization script for RSA based ePassport P	RSA/ConfigApp_Init_P.csf	7	*[8]
17	Pre-Personalization script for RSA ePassport L	RSA/ConfigApp_Pre.csf	8	*[8]
18	Personalization script for RSA ePassport L	RSA/ConfigApp_Person.csf	7	file
19	Constant data for RSA based ePassport	RSA/ConstantData.csf	6	*[8]
20	Configuration data for RSA based Pre-Personalization	RSA/ConfigData_Pre.csf	7	*[8]
21	Configuration data for RSA based Personalization	RSA/ConfigData_Person.csf	8	file
22	Documentation	*CardOS V5.3 Chipcard Operating System, User's Manual*	Dated 05/2014 [11]	PDF
23		*CardOS DI V5.3 Packages & Release Notes*	Dated 10/2015 [24]	PDF
24		*CardOS DI V5.3 ICAO Extension Package Release Notes*	Dated 03/2016 [12]	PDF
25		*Administrator Guidance 'CardOS DI V5.3 EAC/PACE Version 1.0' and 'CardOS DI V5.3 EAC/PACE Version 1.0 (BAC)'*	Version 1.70, dated 2016-06-02 [13]	PDF
26		*User Guidance 'CardOS DI V5.3 EAC/PACE Version 1.0' and 'CardOS DI V5.3 EAC/PACE Version 1.0 (BAC)'*	Version 1.60, dated 2016-03-02 [14]	PDF
27		*ePassport Application 'CardOS DI V5.3 EAC/PACE Version 1.0' and CardOS DI V5.3 EAC/PACE Version 1.0 (BAC)'*	Version 1.30, dated 2016-03-02 [25]	PDF

Table 2: Deliverables of the TOE

---

[8] Not the script files themselves are delivered to the personalization agent but the initialized and pre-personalised inlay created by using these files. For more information, see the following paragraph.

Components no. 1 to no. 5 are actually delivered as one item, namely the IC platform containing the software mask.

Items no. 6 and no. 7 contain patches. These are installed automatically during initialization.

Items no. 8 to no. 21 represent the configuration files for initialization, pre-personalisation and personalization. Here, the script files for physical (P) initialization provide an image based initialization and the script files for logical (L) initialization provide a step by step initialization.

Items no. 8 and no. 9 contain the scripts for EC based initialization.

Items no. 10, no. 12 and no. 13 contain the scripts for EC based pre-personalisation.

Items no. 11 and no. 14 contain the scripts for EC based personalization.

Items no. 15 and no. 16 contain the scripts for RSA based initialization.

Items no. 17, no. 19 and no. 20 contain the scripts for RSA based pre-personalisation.

Items no. 18 and no. 21 contain the scripts for RSA based personalization.

The developer delivers the CardOS DI V5.3 software together with the libraries and the initialisation transport key to the chip manufacturer encrypted through the interface defined in the product certification BSI-DSZ-CC-0782-V2-2015 [15]. The chip manufacturer loads the software in the protected part of the flash EEPROM and protects it with the initialization transport key. The manufactured chips or modules are delivered to the inlay manufacturer by the procedure defined in the product certification BSI-DSZ-CC-0782-V2-2015 [15].

The developer delivers the guidance in electronic form, the CSF files and the initialization transport key by encrypted e-mail to the inlay manufacturer and the personaliser. The modules are initialised and pre-personalised according to the order of the personaliser and secured with the transport keys agreed on between inlay manufacturer and personaliser.

The delivery of the initialized and pre-personalized inlays from the respective inlay manufacturer must be done according to the guidance documentation [13] and [14].

3.   Security Policy

The Security Policy of the TOE is defined according to the MRTD EAC/PACE PP [8] by the Security Objectives and Requirements for the contact-less chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organisation (ICAO). The Security Policy addresses the advanced security methods for authentication and secure communication, which are described in detail in the Security Target [6].

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.Legislative_Compliance: Issuing of the travel document

- OE.Auth_Key_Travel_Document: Travel document Authentication Key

- OE.AA_Key_Travel_Document: Travel document Active Authentication Key

- OE.Authoriz_Sens_Data: Authorization for Use of Sensitive Biometric Reference Data

- OE.Passive_Auth_Sign: Authentication of travel document by signature

- OE.Personalization: Personalization of travel document

- OE.Exam_Travel_Document: Examination of the physical part of the travel document

- OE.Prot_Logical_Travel_Document: Protection of data from the logical travel document

- OE.Ext_Insp_Systems: Authorization of Extended Inspection Systems

- OE.Terminal: Terminal operating

- OE.Travel_Document_Holder: Travel document holder obligations

Details can be found in the Security Target [6], chapter 6.2.

5.   Architectural Information

The TOE is a composite product. It is composed of an integrated circuit, IC dedicated software, the antenna, IC embedded software, and the ePassport application. As all parts of the software run inside the IC, the external interface of the TOE to its environment can be defined as the external interface of the IC, the Infineon SLE78CLFX*P (M7892 B11). For details concerning the CC evaluation of the Infineon IC and its cryptographic libraries see the evaluation documentation under certification ID BSI-DSZ-CC-0782-V2-2015 [15]. According to the TOE Design the Security Functionality of the TOE listed in table 1 is enforced by the following subsystems:

- Protocol Manager (monitors the correct data transfer),

- Command Manager (implements the command identification),

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

- Service Layer (contains service and security routines),

- System Layer (contains system and basic routines),

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

- EPA (ePassport Application), and

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

6.   Documentation

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

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

7.   IT Product Testing

The developer tested all TOE Security Functions either on real cards or with emulator tests. For all commands and functionality tests, test cases are specified in order to demonstrate its expected behaviour including error cases. Hereby a representative sample including all boundary values of the parameter set, e.g. all command APDUs with valid and invalid inputs were tested and all functions were tested with valid and invalid inputs. Repetition of developer tests were performed during the independent evaluator tests. Since many Security Functions can be tested by TR-03110 APDU command sequences, the evaluators performed these tests with real cards. This is considered to be a reasonable approach because the developer tests include a full coverage of all security functionality. Furthermore, penetration tests were chosen by the evaluators for those Security Functions where internal secrets of the card could potentially be modified or observed during testing. During their independent testing, the evaluators covered

- testing APDU commands related to Access Control,
- testing APDU commands related to Identification and Authentication,
- testing APDU commands related to the Secure Messaging Channel,
- source code analysis performed by the evaluators,
- testing the commands which are used to execute the EAC and PACE protocol,
- side channel analysis for SHA, Triple-DES and AES,
- fault injection attacks (laser attacks),
- testing APDU commands for the initialization, personalization and usage phase,
- testing APDU commands for the commands using cryptographic mechanisms, and
- the certification chain verification during Terminal Authentication.

The evaluators have tested the TOE systematically against high attack potential during their penetration testing.

The achieved test results correspond to the expected test results.

8.   Evaluated Configuration

This certification covers the following configurations of the TOE:

- the circuitry of the MRTD's chip (the integrated circuit, IC),
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software,
- the antenna,
- the IC Embedded Software (operating system),
- the ePassport Application, and
- the associated guidance documentation.

The TOE was evaluated in all of its hardware configurations as described in the ST. It can be delivered with different flash sizes and input capacities of the contactless interface:

- SLE78CLFX3000P with 300kByte flash, 27pF,

- SLE78CLFX4000P with 404kByte flash, 27pF,

- SLE78CLFX308AP with 300kByte flash, 78pF,

- SLE78CLFX408AP with 404kByte flash, 78pF.

All derivatives of the smart card IC SLE78CLFX*P (M7892 B11) are certified under ID BSI-DSZ-CC-0782-V2-2015 [15]. The chips can be packaged in modules M8.4, MCC8, MCS8 (27pF) or COM8.6, COM10.6 (78pF) or other modules or packages.

Flash size, input capacity of the contactless interface and the module or package do not have an impact on the TSF of the TOE.

Related to the functionality there are four different configurations and the travel document holder receives only one of these configurations:

- Configuration 1: PACE, CA and TA are EC based,

- Configuration 2: PACE, CA and TA are RSA based,

- Configuration 3: PACE, CA, TA and AA are EC based,

- Configuration 4: PACE, CA, TA and AA are RSA based.

To verify that the user has the correct TOE it can be identified by any entity with the answer to reset (ATR) and with the command GET DATA using specific modes (see Guidance Documents [11], [13] and [14]):

- Answer to reset must contain the version of CardOS DI V5.3 (see No. 3 / 4 in Table 2): "0Bh 3bh D2h 18h 00h 81h 31h FEh 58h C9h 02h 17h".

- GET DATA command with mode 80h must return the product name, version and copyright string "CardOS DI V5.3, 2015": "43h 61h 72h 64h 4fh 53h 20h 044 049 20h 56h 35h 2eh 33h 2ch 20h 32h 30h 31h 35h 00h".

- GET DATA command with mode 8Bh (see [11]) can be used to identify the chip and its answer must match the following pattern:

Index	1	2	…	6	…	11	12	13	14
Value	cch	78h	…	00h	…	00h	01h	0Bh	02h

Table 3: Pattern of the answer to the GET DATA command

- byte 1: "cch"

- byte 2: "78h"

- bytes 3-5: irrelevant

- bytes 6-11: "00h 01h 00h 02h 00h 00h" for SLE78CLFX3000P

- bytes 6-11: "00h 01h 00h 01h 00h 00h" for SLE78CLFX4000P

- bytes 6-11: "00h 01h 00h 70h 00h 00h" for SLE78CLFX308AP

- bytes 6-11: "00h 01h 00h 55h 00h 00h" for SLE78CLFX408AP

- bytes 12-14: "01h 0Bh 02h"

- bytes 15-n: irrelevant

The personalization script files can be identified by a unique version string which can be found in the header of the script files. This version string has to be compared to the strings listed in the Guidance Document [13].

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

● The Application of CC to Integrated Circuits,

● Application of Attack Potential to Smart Cards,

● Composite product evaluation for Smart Cards and similar devices (see AIS 36). 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 [15], [16]) have been applied in the TOE evaluation.

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

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

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 ALC_DVS.2, ATE_DPT.2, AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

● PP Conformance: Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), Version 1.3.2, 05 December 2012, BSI-CC-PP-0056-V2-2012-MA-02 [8]

● for the Functionality: PP conformant
                            Criteria Part 2 extended

● for the Assurance: Common Criteria Part 3 conformant
                            EAL 4 augmented by ALC_DVS.2, ATE_DPT.2, 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

All cryptographic functionalities are described in detail in chapter 10 of the Security Target [6]. The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

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.

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

AA   Active Authentication

AES   Advanced Encryption Standard

AIS   Application Notes and Interpretations of the Scheme

APDU   Application Protocol Data Unit

BAC   Basic Access Control

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   Chip Authentication

CCRA   Common Criteria Recognition Arrangement

CC   Common Criteria for IT Security Evaluation

CEM   Common Methodology for Information Technology Security Evaluation

cPP   Collaborative Protection Profile

DES   Data Encryption Standard; symmetric block cipher algorithm

EAC   Extended Access Control

EAL   Evaluation Assurance Level

ECC   Elliptic Curve Cryptography

ETR   Evaluation Technical Report

ICAO	International Civil Aviation Organisation
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MAC	Message Authentication Code
MRTD	Machine Readable Travel Document
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
RNG	Random Number Generator
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SM	Secure Messaging
ST	Security Target
TA	Terminal Authentication
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

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

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.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

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 - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

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
       http://www.commoncriteriaportal.org

[2]   Common Methodology for Information Technology Security Evaluation (CEM),
       Evaluation Methodology, Version 3.1, Rev. 4, September 2012,
       http://www.commoncriteriaportal.org

[3]   BSI certification: Scheme documentation describing the certification process
       (CC-Produkte) and Scheme documentation on requirements for the Evaluation
       Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4]   Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[9]
       https://www.bsi.bund.de/AIS

[5]   German IT Security Certificates (BSI 7148), periodically updated list published also
       on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6]   Security Target BSI-DSZ-CC-0967-2016, Version 2.01, 19.04.2016, Security Target
       'CardOS DI V5.3 EAC/PACE Version 1.0', Atos IT Solutions and Services GmbH

[7]   Evaluation Technical Report, Version 6, 20.06.2016, Evaluation Technical Report
       Summary (ETR Summary) CardOS DI V5.3 EAC/PACE Version 1.0, TÜV
       Informationstechnik GmbH (confidential document)

[8]   Protection Profile Machine Readable Travel Document with "ICAO Application"
       Extended Access Control with PACE, Version 1.3.2, 5 December 2012,
       BSI-CC-PP-0056-V2-2012-MA-02, BSI

[9]   Protection Profile Machine Readable Travel Document using Standard Inspection
       Procedure with PACE (PACE PP), Version 1.0, 2 November 2011,
       BSI-CC-PP-0068-V2-2011, BSI

---

[9]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 EAL 5+ (CCv2.3 &
  CCv3.1) and EAL 6 (CCv3.1)

- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and
  CC Supporting Document and CCRA policies

- AIS 36, Version 4, Kompositionsevaluierung including JIL Document and CC Supporting Document

- AIS 38, Version 2, Reuse of evaluation results

[10]   Configuration list for the TOE, Version 1.30, 03.06.2016, Configuration List 'CardOS DI V5.3 EAC/PACE Version 1.0' and 'CardOS DI V5.3 EAC/PACE Version 1.0 (BAC)', Atos IT Solutions and Services GmbH (confidential document)

[11]   Guidance documentation for the TOE, Version 05/2014, CardOS V5.3 Chipcard Operating System, User's Manual, Atos IT Solutions and Services GmbH

[12]   Guidance documentation for the TOE, Version 03/2016, CardOS DI V5.3 ICAO Extension Package Release Notes, Atos IT Solutions and Services GmbH

[13]   Guidance documentation for the TOE, Version 1.70, 02.06.2016, Administrator Guidance 'CardOS DI V5.3 EAC/PACE Version 1.0' and 'CardOS DI V5.3 EAC/PACE Version 1.0 (BAC)' , Atos IT Solutions and Services GmbH

[14]   Guidance documentation for the TOE, Version 1.60, 02.03.2016, User Guidance 'CardOS DI V5.3 EAC/PACE Version 1.0' and 'CardOS DI V5.3 EAC/PACE Version 1.0 (BAC)' , Atos IT Solutions and Services GmbH

[15]   Certification Report, BSI-DSZ-CC-0782-V2-2015, 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), v1.0, 2015-11-03, BSI.

[16]   ETR for composite evaluation, M7892 B11, Certification ID: BSI-DSZ-CC-0782-V2-2015, Version 7, 2015-10-21, TÜViT

[17]   Machine Readable Travel Documents Technical Report, Supplemental Access Control for Machine Readable Travel Documents, International Civil Aviation Organization, Version 1.00, 11 November 2010

[18]   ICAO, Machine Readable Travel Documents, Part 1 - Machine Readable Passports. International Civil Aviation Organization, 2006

[19]   ICAO, Machine Readable Travel Documents, Part 3 - Machine Readable Official Travel Documents. International Civil Aviation Organization, 2008

[20]   Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20.03.2012, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[21]   Machine Readable Travel Documents Technical Report, PKI for Machine Readable Travel Documents Offering ICC Read-Only Access, Version 1.1, 01.10.2004, published by authority of the secretary general, International Civil Aviation Organization

[22]   Certification Report, BSI-DSZ-CC-S-0056-2015 for HID Global Ireland Teoranta, Pairc Tionscail naTulaigh, Baile na hAbhann, Co. Galway, Ireland (Building B1, B2, B3) of HID Global Ireland Teoranta, 02.10.2015, BSI

[23]   Certification Report, BSI-DSZ-CC-S-0057-2015 for Inlay Production and Initialisation of SMARTRAC Site Bangkok of SMARTRAC TECHNOLOGY Ltd., Bangkok, Thailand, 28.12.2015, BSI

[24]   Guidance documentation for the TOE, Version 10/2015, CardOS DI V5.3 Packages & Release Notes, Atos IT Solutions and Services GmbH

[25]   Guidance documentation for the TOE, Version 1.30, 02.03.2016, ePassport Application 'CardOS DI V5.3 EAC/PACE Version 1.0' and 'CardOS DI V5.3 EAC/PACE Version 1.0 (BAC)', Atos IT Solutions and Services GmbH

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
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

Assurance Class	Assurance Components
	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.

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

"Objectives

EAL 1 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.

EAL 1 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.

EAL 1 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 EAL 1 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 (EAL 2) - structurally tested (chapter 8.4)

"Objectives

EAL 2 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.

EAL 2 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 (EAL 3) - methodically tested and checked (chapter 8.5)

"Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 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 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 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. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 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 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 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 EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 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 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 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.

EAL 6 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 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 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 EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
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"

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."

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-0967-2016

Evaluation results regarding development and production environment

The IT product CardOS DI V5.3 EAC/PACE Version 1.0 (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 23 June 2016, 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.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2)

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 München, Germany (Development)

    b)   Atos IT Solutions and Services GmbH, Würzburger Str. 121, 90766 Fürth, Germany (Development)

    c)   Atos IT Solutions and Services GmbH, Lohberg 10, 49716 Meppen, Germany (Development)

    d)   Atos IT Solutions and Services d.o.o., Zrinsko-Frankopanska 64, 21000 Split, Croatia (Development)

    e)   HID Global, Pairc Tionscail na Tulaigh, Baile na hAbhann, Galway, Ireland, BSI-DSZ-CC-S-0056-2015 [22] (Initialization, Pre-Personalization, Inlay Manufacturing)

    f)   SmarTrac Technology Ltd, 142/121/115 Moo, Hi-Tech Industrial Estate Tambon Ban Laean, Amphor Bang-pa-in 13160 Ayutthaya, Thailand, BSI-DSZ-CC-S-0057-2015 [23] (Initialization, Pre-Personalization, Inlay Manufacturing)

For development and production sites regarding the platform please refer to the certification report BSI-DSZ-CC-0782-V2-2015 [15].

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.