Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1172-2022

for

CardOS V6.0 ID R1.0 (BAC)

from

Atos Information Technology 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-1172-2022 (*)

CardOS V6.0 ID R1.0 (BAC)

from	Atos Information Technology GmbH
PP Conformance:	Machine Readable Travel Document with "ICAO Application" Basic Access Control, Version 1.10, 25 March 2009, BSI-CC-PP-0055-2009
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_DVS.2

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 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 5.

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
recognition for components
up to EAL 2 and ALC_FLR
only

Bonn, 11 March 2022

For the Federal Office for Information Security

Sandro Amendola
Head of Division

L.S.

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

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.

Contents

A. Certification

1. 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.

2. 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[1]
- BSI Certification and Approval Ordinance[2]
- BMI Regulations on Ex-parte Costs [3]
- 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[4] [1] also published as ISO/IEC 15408.

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

2 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

3 BMI Regulations on Ex-parte Costs - Besondere Gebührenverordnung des BMI für individuell zurechenbare öffentliche Leistungen in dessen Zuständigkeitsbereich (BMIBGebV), Abschnitt 7 (BSI-Gesetz) - dated 2 September 2019, Bundesgesetzblatt I p. 1365

- 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]

3. 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.

3.1. European Recognition of 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.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. 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 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.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

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

3.2. 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 current list of signatory nations and approved certification schemes can be seen on the website: https://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 related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ ALC_FLR components.

[4] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

4. 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 V6.0 ID R1.0 (BAC) has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-1162-2021. Specific results from the evaluation process BSI-DSZ-CC-1162-2021 were re-used.

The evaluation of the product CardOS V6.0 ID R1.0 (BAC) was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 3 February 2022. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Atos Information Technology GmbH.

The product was developed by: Atos Information Technology GmbH.

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

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is 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 components and assurance levels please refer to CC itself. Detailed references are listed in part C of this 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-assessment or 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 would 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 11 March 2022 is valid until 10 March 2027. 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

[5] 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.

6. Publication

The product CardOS V6.0 ID R1.0 (BAC) 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[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Atos Information Technology 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 composite TOE is named CardOS V6.0 ID (BAC) R1.0 and was developed by Atos Information Technology GmbH. The TOE is a smart card operating system on an IC with one application. Applications covered by this TOE comprise the electronic passport (ePass) application. The TOE is a machine readable travel document based on the requirements of ICAO which can be accessed through the contact-based and contactless interface of the TOE. It supports Basic Access Control (BAC) only and is a re-evaluation of CardOS V6.0 ID R1.0, certified as BSI-DSZ-CC-1162-2021.

The IC platform comprises the integrated circuit SLC52GDA448* (IFX_CCI_000005 Design Step H13) and the cryptographic libraries RSA v2.08.007, EC v2.08.007, Toolbox v2.08.007, Base v2.08.007, HCL2 v1.12.001 (hash library) and Symmetric Crypto Library (SCL) v2.04.002 certified according CC v3.1 with ID BSI-DSZ-CC-1110-V4-2021.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile [8].

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.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 7.1. 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
User Identification and Authentication (BAC)
BAC protocol
Read access to the LTD and SO.D at phase Operational Use
Secure messaging
Test features
Protection

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 8.1.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 4.1. 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 4.2, 4.3 and 4.4.

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 V6.0 ID R1.0 (BAC)

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	Infineon SLC52GDA448*	IFX_CCI_000005 Design Step H13	Wafer, module or a packaged component.
2	SW	CardOS V6.0 ID R1.0	V.60 / R1.0	
3	SW (Infineon)	RSA Library	v2.08.007	
4		EC Library	v2.08.007	
5		Toolbox Library	v2.08.007	
6		Base Library	v2.08.007	
7		Hash Library	v1.12.001	
8		Symmetric Crypto Library	v2.04.002	
9	DOC	CardOS V6.0 User's Manual	08/2021	As PDF via signed and encrypted mail.
10		User Guidance 'CardOS V6.0 ID R1.0' and 'CardOS V6.0 ID R1.0 (BAC)'	1.20R	
11		Administrator Guidance 'CardOS V6.0 ID R1.0' and 'CardOS V6.0 ID R1.0 (BAC)'	1.31R	
12		Application Base Guidance 'CardOS V6.0 ID R1.0' and 'CardOS V6.0 ID R1.0 (BAC)'	1.33R	
13		Application ePassport Guidance 'CardOS V6.0 ID R1.0' and 'CardOS V6.0 ID R1.0 (BAC)'ePassport Guidance 'CardOS V6.0 ID'	1.32R	
14		Application eSign Guidance 'CardOS V6.0 ID R1.0' and 'CardOS V6.0 ID R1.0 (BAC)'	1.22R	
15	DATA	Configuration Scripts for initialization and personalization	R1.03	As PDF via signed and encrypted mail.
16		StartKey for initialization	-	

Table 2: Deliverables of the TOE

Components No. 1 to No. 8 are actually delivered as one item, namely the IC platform containing the software mask.

Item No. 15 represents the configuration files for initialization and personalization. These represent possible configurations and changes on values and parameters can be applied as outlined in the scripts itself and according to the guidance documents.

The OS software pre-loaded on the IC hardware is sent directly from the chip manufacturer to the Trust Center or via logistic centers or distributors. This is possible since the TOE protects itself during delivery and standard procedures for packing, storage and distribution can be applied. Only with knowledge of the StartKey it is possible to continue the process of setting up the TOE. The Trust Center is also provided with the guidance and initialization / personalization scripts from the developer Atos Information Technology GmbH. All data and documents are sent signed and encrypted by mail.

The TOE can be identified in accordance with the described processes in Administrator Guidance chap. 5.1, User Guidance chap. 4.2 and Application Base Guidance chap. 4.1 [12]. After the delivery the TOE can be identified by the command response sequence as outlined in Application Base Guidance chap. 4.1 and Administrator Guidance chap. 5.1 [12], verifying the OS version, product name, version and year, chip identification and loaded packages (i.e. none in this case).

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:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF

Specific details concerning the above mentioned security policies can be found in Chapter 7 of 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.MRTD_Manufact (Protection of the MRTD Manufacturing)
- OE.MRTD_Delivery (Protection of the MRTD delivery)
- OE.Personalization (Personalization of logical MRTD)
- OE.Pass_Auth_Sign (Authentication of logical MRTD by Signature)
- OE.BAC-Keys (Cryptographic quality of Basic Access Control Keys)
- OE.Exam_MRTD (Examination of the MRTD passport book)
- OE.Passive_Auth_Verif (Verification by Passive Authentication)

- OE.Prot_Logical_MRTD (Protection of data from the logical MRTD)

Details can be found in the Security Target [6], chapter 5.2.

5. Architectural Information

The composite TOE CardOS V6.0 ID (BAC) R1.0 is a smart card operating system based on a certified hardware platform together with the cryptographic libraries and object system that defines its applications. The TOE comprises ten subsystem, listed with a short description in the following itemization:

- Startup: Performs actions needed at startup only and not further used after entry into user commands processing loop.
- Command Manager: The main loop within the Command Manager is the most central part of CardOS.
- Protocol Manager: The Protocol Manager takes care of command reception and transmission of response data.
- Command Layer: Implements the APDU command set, enables secure access to data and allows for package download.
- Security: Selects appropriate rules and the corresponding evaluation, manages the administration of access rights, provides secure messaging processing, evaluates an entities life cycle when influencing access rules, protects the TOE against attacks using the underlying hardware security features.
- Entities: Provides the mediation of access to the application and its objects, provides file system administration, setting of authorization flags, provides PIN/PUK blocking functionality, handles private keys for signature generation with appropriate parameters, handles SCP functionality, provides integrity mechanisms (CRC), checks file status and provides countermeasures against fault induction attacks.
- Cryptography: Provides wrapper modules for IFX platform libraries, padding routines and generic management of cryptography.
- CBIOS: Provides interface functionality to the hardware peripherals (UART, CRC generator) and provides utility functions (memory management, transaction management, interrupt service routines).
- IC: Represents the parts of the underlying hardware platform of the composite TOE, which interacts with the operating system.
- Retrieval functions: This subsystem retrieves the results of performed routines.

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

Developer's Test according to ATE_FUN

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 main test focus was laid upon the access right management and commands and that are used in the operational usage phase to allow signature creation. Tests using multiple application DFs to verify their separation were performed.

Additional test cases that could not be performed on a real smartcard (e.g. memory faults and manipulation) were performed on an 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 configuration options as described in the ST are covered and a well-defined approach of possible combinations of options was applied. All test results collected in the test reports are as expected and in accordance with the TOE design and the desired TOE functionality.

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 using developer’s and evaluator’s test equipment.

TOE test configurations:

- Tests were done in different life-cycle phases (personalisation / operational),
- eSign and ePassport application, combinations of both applications and multiple instances were considered in the product test configurations,
- Different options on application parameters were tested, for example RSA or EC-based cryptography (Brainpool and NIST curves), different key lengths or PIN/PUK options (not BAC-related however).

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 ST. Access control and user authentication was mainly in focus.
- Penetration tests as outcome of the vulnerability analysis were performed to cover potential vulnerabilities. Fuzzy tests, laser fault injections and side-channel analysis were conducted during testing.

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.

Penetration Testing according to AVA_VAN

Overview:

The penetration testing was performed at the site of the evaluation body TÜViT in the evaluator's test environment with the evaluator's test equipment. The samples were provided by the sponsor and developer. The test samples were configured and parameterized by the evaluator according to the guidance documentation. The single configuration of the TOE intended to be covered by the current evaluation was tested. The overall result is that no deviations were found between the expected result and the actual result of the tests. Moreover, no attack scenario with an attack potential of Enhanced-Basic was actually successful.

Penetration testing approach:

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment created within the vulnerability analysis evaluation report, the evaluator created attack scenarios for the penetration tests, where the evaluator is of the opinion that the vulnerabilities could be exploitable. While doing so, the evaluator also considered all aspects of the security architecture of the TOE being not covered by the functional developer tests.

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 supported testing activity by enabling the evaluator to verify implementation aspects that could hardly be covered by test cases.

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

TOE test configurations:

The evaluators used TOE samples for testing that were configured according to the ST and guidance documentation. The samples were identified using the method as described by the developer in its guidance documentation. Both, contactless and contact based interface were covered during testing.

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 Enhanced-Basic was actually successful in the TOE's operational environment as defined in [ST] provided that all measures required by the developer are applied.

Summary of Test Results and Effectiveness Analysis

The test results yielded 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 [6] provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The tests were performed with the composite smartcard product CardOS V6.0 ID R1.0 (BAC) on the IC SLC52GDA448* (IFX_CCI_000005 Design Step H13). The developer tested the TOE on a product with additional eID functionality, which is outside of the TOE scope, using a wide spectrum of configurations, and configuration parameters basically categorized as follows:

- Configuration variants with ECC ePassport application,
- Configuration variants with RSA ePassport application,
- Configuration variants with eSign and ePassport applications:
  - Both ECC-based,
  - Both RSA-based,
  - One ECC-based and one RSA-based, and
  - A 4th configuration with ECC and RSA vice versa.

A special test configuration was used for test cases where the TOE shall be in the MANUFACTURING card life cycle before delivery. The tested configurations take into account the configurable options of the eID product (CardOS V6.0 ID / BSI-DSZ-CC-1162) as e.g. the use of elliptic curves or RSA, different key lengths, use of Brainpool or NIST elliptic curves, contact and contactless interface, and other options related to PIN secrets or Active Authentication.

All configurations were tested appropriately with a similar amount of tests. The tests were performed in all life-cycle phases that are in scope after TOE delivery within the according operation environment.

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 EAL 5 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:

(i) AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers

(ii) *AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)*

(iii) *AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)*

(iv) *AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren*

(v) *AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document*

(vi) *AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema*

(vii) *AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)*

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

(ix) *AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document*

(x) *AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen*

(xi) *AIS 45, Version 2, Erstellung und Pflege von Meilensteinplänen*

(xii) *AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren*

For smart card specific methodology the scheme interpretations AIS 26 and AIS 36 were 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 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-1162-2021, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on BAC specific TOE parts.

The evaluation has confirmed:

- PP Conformance: Machine Readable Travel Document with "ICAO Application" Basic Access Control, Version 1.10, 25 March 2009, BSI-CC-PP-0055-2009 [8]
- for the Functionality: PP conformant
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_DVS.2

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 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).

The table A.1 presented in the Security Target gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view.

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 and his system risk management process, too.

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. Regulation specific aspects (eIDAS, QES)

None.

13. Definitions

13.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
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
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation

CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

13.2. 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.

14. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://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[7] 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-1172-2022, Version 1.35R, 2021-11-19, Security Target 'CardOS V6.0 ID R1.0 (BAC)', Atos Information Technology GmbH

[7] Evaluation Technical Report BSI-DSZ-CC-1172, Version 2, 2022-02-03, EVALUATION TECHNICAL REPORT SUMMARY (ETR SUMMARY), TÜV Informationstechnik GmbH, (confidential document)

[8] Machine Readable Travel Document with "ICAO Application" Basic Access Control, Version 1.10, 25 March 2009, BSI-CC-PP-0055-2009

[7] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 14, Version 7, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 19, Version 9, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria)
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for 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 5, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 37, Version 3, Terminologie und Vorbereitung von Smartcard-Evaluierungen
- AIS 45, Version 2, Erstellung und Pflege von Meilensteinplänen
- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[9] Certification Report – BSI-DSZ-CC-1110-V4-2021 for Infineon Security Controller IFX_CCI_000003h, 000005h, 000008h, 00000Ch, 000013h, 000014h, 000015h, 00001Ch, 00001Dh, 000021h, 000022h in the design step H13 and including optional software libraries and dedicated firmware in several versions from Infineon Technologies AG, BSI

[10] ETR FOR COMPOSITE EVALUATION (ETR-COMP), IFX_CCI_000003h, IFX_CCI_000005h, IFX_CCI_000008h, IFX_CCI_00000Ch, IFX_CCI_000013h, IFX_CCI_000014h, IFX_CCI_000015h, IFX_CCI_00001Ch, IFX_CCI_00001Dh, IFX_CCI_000021h, IFX_CCI_000022h H13, BSI-DSZ-CC-1110-V4, Version 1, 2021-07-01, TÜViT (confidential document)

[11] Configuration list for the TOE, Version 1.33, 2022-02-03, Configuration List ’CardOS V6.0 ID R1.0’ and ’CardOS V6.0 ID R1.0 (BAC)’, Atos Information Technology GmbH (confidential document)

[12] Guidance documentation for the TOE (confidential documents)

CardOS V6.0 User’s Manual, 08/2021, Atos Information Technology GmbH

User Guidance ’CardOS V6.0 ID R1.0’ and ’CardOS V6.0 ID R1.0 (BAC)’, Revision 1.20R, 2021-10-21, Atos Information Technology GmbH

Administrator Guidance ’CardOS V6.0 ID R1.0’ and ’CardOS V6.0 ID R1.0 (BAC)’, Revision 1.31R, 2021-10-25, Atos Information Technology GmbH

Application Base Guidance ’CardOS V6.0 ID R1.0’ and ’CardOS V6.0 ID R1.0 (BAC)’, Revision 1.33R, 2021-10-21, Atos Information Technology GmbH

Application ePassport Guidance ’CardOS V6.0 ID R1.0’ and ’CardOS V6.0 ID R1.0 (BAC)’ePassport Guidance ’CardOS V6.0 ID’, Revision 1.32R, 2021-10-21, Atos Information Technology GmbH

Application eSign Guidance ’CardOS V6.0 ID R1.0’ and ’CardOS V6.0 ID R1.0 (BAC)’, Revision 1.22R, 2021-10-21, Atos Information Technology GmbH

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailed definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at https://www.commoncriteriaportal.org/cc/

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

Annex B of Certification Report BSI-DSZ-CC-1172-2022

Evaluation results regarding development and production environment

The IT product CardOS V6.0 ID R1.0 (BAC) (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 Scheme Interpretations by advice of the Certification Body for components beyond EAL 5 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 11 March 2022, 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.2, ALC_LCD.1, ALC_TAT.1)

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

a) Atos Information Technology GmbH, Otto-Hahn-Ring 6, 81739 Munich, Germany (SW Development)

b) Atos Information Technology GmbH, Wuerzburger Str. 121, 90766 Fuerth, Germany (SW Development)

c) Atos IT Solutions and Services d.o.o, Matice Hrvatske 15, 21000 Split, Croatia (SW Development)

d) See [9] for the development and production sites of the hardware platform.

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.

Note: End of report