Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1176-2023

for

PWPW SmartApp-MRTD 1.0

from

Polska Wytwórnia Papierów Wartościowych S.A.

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-1176-2023 (*)

PWPW SmartApp-MRTD 1.0

from	Polska Wytwórnia Papierów Wartościowych S.A.
PP Conformance:	Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), Version 1.3.2, 5 December 2012, BSI-CC-PP-0056-V2-2012-MA-02, Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP), Version 1.01, 22 July 2014, BSI-CC-PP-0068-V2-2011-MA-01
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ATE_DPT.2, ALC_DVS.2 and AVA_VAN.5

SOGIS Recognition Agreement

Common Criteria

Common Criteria Recognition Arrangement recognition for components up to EAL 2 only

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 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.

Bonn, 22 May 2023

For the Federal Office for Information Security

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

Matthias Intemann L.S.
Head of Branch

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 und für Heimat (Federal Ministry of the Interior and Community)
- 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.

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

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

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 PWPW SmartApp-MRTD 1.0, has undergone the certification procedure at BSI.

The evaluation of the product PWPW SmartApp-MRTD 1.0, was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 30 March 2023. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the applicant is: Polska Wytwórnia Papierów Wartościowych S.A..

The product was developed by: Polska Wytwórnia Papierów Wartościowych S.A..

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 22 May 2023 is valid until 21 May 2028. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

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 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 PWPW SmartApp-MRTD 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[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Polska Wytwórnia Papierów Wartościowych S.A.
1 Sanguszki St.
00-222 Warsaw
Poland

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 composite TOE named PWPW SmartApp-MRTD and has been evaluated in version 1.0. The TOE is an electronic travel document representing a contactless smart card. The TOE provides cryptographic services according to the protection profiles [8].

The PWPW SmartApp-MRTD 1.0 comprises of:

- the hardware (microcontroller, the integrated circuit, IC),
- the native implementation of the e-passport,
- the guidance documentation.

The Composite TOE is provided by Infineon through the delivery channel certified in scope of the IC certification BSI-DSZ-CC-1110-V5-2022-MA-01.

The TOE supports the following security protocols/mechanisms specific for travel documents:

1. PACE or PACE with CAM,
2. Extended Access Control, i.e.:
   - Chip Authentication,
   - Terminal Authentication,
3. Passive Authentication.

Passive Authentication data is calculated by the TOE environment and stored securely in the TOE during its personalization.

The TOE comprises of at least:

- the circuitry of the travel document’s chip (the integrated circuit, IC);
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software;
- the IC Embedded Software (application) and
- the associated guidance documentation.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profiles Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), Version 1.3.2, 5 December 2012, BSI-CC-PP-0056-V2-2012-MA-02,
Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP), Version 1.01, 22 July 2014, BSI-CC-PP-0068-V2-2011-MA-01 [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 ATE_DPT.2, ALC_DVS.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. 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:

Identifier	Security functionalities and features
SF.MRTD	The security functionality provides the mechanism, which allows to control the TOE life cycle phases, check user roles and enforce national and/or international security policies relevant for the travel documents.
SF.CRYPTO	The security functionality generates random challenges intended for various authentication mechanisms.
SF.SAUTH	The security functionality concerts symmetric authentication mechanism as well as it allows replacing the existing authentication key.
SF.PACE	The security functionality authenticates the inspection system, which tries to establish connection with the TOE.
SF.SM	The security functionally is used to secure communication between the TOE and the Personalization Agent or the TOE and the inspection system.
SF.CA	Chip Authentication is used by the TOE to prove its identity (to prevent cloning).
SF.TA	Terminal authentication is used to authenticates the inspection system.
SF.SEC	Hardware security protection.
SF.CONF	The security functionality is used to configure the application with the e-passport functionality.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. 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 3.3 to 3.5.

This certification covers the configurations of the TOE as outlined in chapter 8 of this report.

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:

PWPW SmartApp-MRTD 1.0,

The following tables outline the TOE deliverables:

No.	Type	Item / Identifier	Release / Version	Form of Delivery
1	SW	PWPW SmartApp-MRTD application	1.0.44.0	PGP encrypted software data from PWPW via internet portal SecureX to IFX.

Table 2: TOE Deliverables for IC manufacturer Infineon

No.	Type	Item / Identifier	Release / Version	Form of Delivery
1	HW/SW	PWPW SmartApp-MRTD composite product on certified Infineon IC	1.0.44.0	The Composite TOE is provided by Infineon through the delivery channel certified in scope of the IC certification BSI-DSZ-CC-1110-V5-2022-MA-01.
2	DOC	*PWPW SmartApp-MRTD 1.0: Preparative procedures*	1.0.11.0	PGP encrypted and public key certificate authenticated from PWPW to personalization agent.
3	DOC	*PWPW SmartApp-MRTD 1.0: Operational user guidance*	1.0.9.0	PGP encrypted and public key certificate authenticated from PWPW to personalization agent.
4	DATA	*Personalization Agent Key and its identifier*	-	Delivered to the personalization agent via extranet portal of Infineon – CC SecureX.
5	DATA	*Secure Messaging seed material*	-	Delivered to the personalization agent via extranet portal of Infineon – CC SecureX.

Table 3: TOE Deliverables for travel document manufacturer

The developer states, that effectively no delivery to customers will take place for the certified TOE and delivery procedures. More so, 1.3.4.2 of the Security Target [6] identifies the travel document manufacturer as the only client. Likewise, Infineon (IFX by ST [6]) is identified as the only (unique) client and customer for the delivery of the MRTD App from the developer, with the procedures certified for the Infineon IC the composite TOE is based on. The delivery of the composite TOE, consisting of the Application integrated on the certified IC, is then delivered via the delivery channels certified in scope of the HW IC certification. The IC manufacturer Infineon locks the Flash Loader during the manufacturing process which will permanently disable the ability to reload or delete the Embedded Software.

Delivery of guidance documents for personalization are delivered from PWPW to the personalization agent as a pgp encrypted and signed file.

The TOE can be identified in accordance with the described processes in chapter 3 of [10]. The application version and its state can verified using the GET DATA (Version) command as described in chapter 3.2 of [10].

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:

- Key management,
- Key generation,
- Data encryption,
- Authentication and attestation of the TOE, trusted channel,
- Identification and authentication,
- Access control,
- User data protection
- Security Audit,
- Security management, and
- Protection of the security features.

Specific details concerning the above mentioned security policies can be found in Chapter 6.1 and 6.2 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.Legislative_Compliance: Issuing of the travel document,
- OE.Passive_Auth_Sign: Authentication of travel document by Signature,
- OE.Personalization: Personalization of travel document,
- OE.Terminal: Terminal operating,
- OE.Travel_Document_Holder: Travel document holder Obligations,
- OE.Auth_Key_Travel_Document: Travel document Authentication Key,
- OE.Authoriz_Sens_Data: Authorization for Use of Sensitive Biometric Reference Data,
- 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.

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

5. Architectural Information

The TOE comprises the following subsystems:

- mrtd: Subsystem mrtd ensures the MRTD application functionality. It controls all primary subsystems. Based on established protocols and application's lifecycle, the subsystem decides to permit or discard each operation and gives or discards access to the sensitive data.
- conf: Subsystem conf is used to configure the MRTD application behavior. It allows to configure the following: communication interface, used protocols and operating system behavior (i.e. deactivate Flash Loader, disable chip serial number).
- fs: Subsystem fs has access to the nonvolatile memory NVM and stores information of each file localization, size, identifier and security conditions. It allows creating, deleting, erasing, updating and reading specified files. The subsystem also allows to select the Master File as well as the MRTD application.
- sauth: Subsystem sauth ensures the personalization agent functionality. It allows the following operations: changing personalization agent key, changing personalization agent key identifier, changing secure messaging seed (used to derivate secure messaging keys which are used during configuration, pre-personalization and personalization), enabling personalization Agent secure login and switch to the next life cycle phase. The operational phase is the last phase in the application. PA (Personalization Agent) is permanently disabled in the operational phase.
- ta: Subsystem ta is responsible for the terminal authentication protocol. It allows the following: reading and validating certificates, loading CVCA certificates, updating CV-Link certificates and TA protocol establishment.
- ca: Subsystem ca is responsible for the Chip Authentication protocol. It allows CA protocol establishment and stores additional information used by the ta subsystem, i.e. the X-coordinate of the terminal's public key.
- pace: Subsystem pace is responsible for the Password Authentication Connection Establishment (PACE) protocol. It allows PACE protocol establishment and stores additional information used by the ta subsystem, i.e. Id PICC - defined as the X coordinate of the ephemeral PACE public key.
- test: Subsystem test is used only during testing life cycle to verify the syntax of all supported APDU commands as well as to perform proprietary internal tests. It is used to test the following subsystems: crypto, sec and nvm. The subsystem is used only in the development phase. For operational usage, the subsystem is permanently removed from the application execution code.
- sm: Subsystem sm performs secure messaging operations. It is used to perform the following operations: converting command in plain text to its protected representation and converting protected command to the command in plain text. Moreover, the subsystem verifies the integrity of protected commands.
- gc: Subsystem gc is used to recover the NVM after file deletion. The subsystem is able to move files inside the memory, to achieve bigger memory space for the new file.
- main: Subsystem main is a representation of the application main entry. The following operations are performed in the subsystem: application configuration, verification of the security measures and execution of the mrtd subsystem.
- apdu: Subsystem apdu performs conversion from received raw bytes into the APDU

structure. The structure contains following fields: class byte, instruction byte, P1 parameter byte, P2 parameter byte, data length, response length, APDU's case and information if command or response was split into parts. The APDU structure is used by executive methods dedicated for specified APDUs.

- timer: Subsystem timer is used to configure internal timers available in microcontroller. Timers are used by proto subsystem, com subsystem and pace subsystem.
- ram: Subsystem ram is used to manage RAM. It performs the following operations: setting memory pool, allocating and freeing memory.
- crypto: Subsystem crypto is a one common interface for all functionalities related to the cryptographic operations. There were specified three groups of such functionalities: cryptographic operations realized with crypto library support, operations realized with SCP support and proprietary operations realized by PWPW, which are: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 and RetailMac, CMAC. RetailMac and CMAC are realized based on SCP and proprietary implementation.
- nvm: Subsystem nvm is used to manage nonvolatile memory NVM. It allows the following operations: reading data, writing data, filling specified memory range with solid data values, setting additional variable key for more secured memory areas, configuring and processing data recovery on accidental power cut.
- reg: Subsystem reg is a wrapper for operations on microcontroller registers.
- sec: Subsystem sec ensures the application security. It is used to perform the following operations: flow counter management, sensitive data management and interception of critical exceptions reported by the hardware.
- imm: Subsystem imm is used to manage and control communication interfaces – contact base and contactless. It controls based on configuration settings which interface should be available: only contact based, only contactless or both interfaces.
- proto: Subsystem proto is used to control communication protocol correctness and its flow. It supports the following communication protocols: T=0, T=1 and T=CL. For contactless communication this subsystem is the only entry point for the outside world, which enables the terminal to ex-change data with the MRTD application.
- com: Subsystem com ensures contact based communication. For contact based communication this subsystem is the only entry point for the outside world, which enables the terminal to exchange data with the MRTD application.

6. Documentation

The evaluated documentation as outlined in table 3 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

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

7. IT Product Testing

7.1. Developer's Test according to ATE_FUN

TOE configurations:

- RELEASE firmware,
- DEBUG firmware (available only during development phase), and
- TEST firmware (available only during development phase).

Developer test suites:

- PWPW-SCrdUVXTester,
- GoogleTest Framework, and
- Keolabs SCRIPTIS.

Testing approach:

- Automatically executed tests within test suites,
- Each line of code is mapped to one test (APDU or GoogleTest),
- Coverage and depth analysis by mapping of the test cases to the code (i.e. subsystems and interfaces of the TOE), and
- APDU tests split in scenarios, test cases and steps.

The developer’s testing efforts have been proven sufficient to demonstrate that the TSFIs and subsystems perform as expected.

7.2. Evaluator Tests - Independent Testing according to ATE_IND

In the following the evaluator’s independent testing efforts are summarized:

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.
- During sample testing the evaluator chose to repeat all developer functional tests at the Evaluation Body for IT Security in Essen.
- 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.
- The evaluator repeated all tests of the developer’s testing documentation, therefore no sampling strategy was applied.

Verdict for the activity:

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

7.3. Evaluator Tests - 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 developer. The test samples were configured and parameterized by the evaluator according to the guidance documentation. The one configuration of the TOE being 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 High was actually successful.

Penetration testing approach:

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment created within 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 tests were performed with the one configuration of the TOE as stated in the security target.

Verdict for the sub-activity:

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

8. Evaluated Configuration

The evaluated TOE configuration is identical with the one described in part B., Chapter 1 of this report, which in turn is the delivered product. There is only one configuration of the TOE. For all tests the TOE is configured and parameterized, if necessary, according to the guidance documents.

The TOE needs to be initialized, configured, personalized and operated according to the guidance documentation.

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) Composite product evaluation for Smart Cards and similar devices according to AIS 36 (see [4]). According to this concept the relevant guidance documents of the underlying platform and the documents ETR for Composition from the platform evaluations [19, 20] have been applied in the TOE evaluation.

(ii) Guidance for Smartcard Evaluation (AIS 37, see [4]).

(iii) Attack Methods for Smartcards and Similar Devices (AIS 26, see [4]).

(iv) Application of Attack Potential to Smartcards (AIS 26, see [4]).

(v) Application of CC to Integrated Circuits (AIS 25, see [4]).

(vi) Security Architecture requirements (ADV_ARC) for smart cards and similar devices (AIS 25, see [4]).

(vii) Evaluation Methodology for CC Assurance Classes for EAL5+ and EAL6 (AIS 34, see [4])

(viii) Functionality classes and evaluation methodology of physical and deterministic random number generators (AIS 20 and AIS 31, see [4]).

(ix) Informationen zur Evaluierung von kryptographischen Algorithmen (AIS 46, see [4]).

For smart card specific methodology the scheme interpretations AIS 25, AIS 26, AIS 34, AIS 36, AIS 37 and AIS 46 (see [4]) were used. For RNG assessment the scheme interpretations AIS 20 and AIS 31 were used (see [4]).

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

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

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

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ATE_DPT.2, ALC_DVS.2 and 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, 5 December 2012, BSI-CC-PP-0056-V2-2012-MA-02, Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP), Version 1.01, 22 July 2014, BSI-CC-PP-0068-V2-2011-MA-01 [8]
- for the Functionality: PP conformant plus product specific extensions Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant EAL 4 augmented by ATE_DPT.2, ALC_DVS.2 and AVA_VAN.5

For specific evaluation results regarding the development and production environment see annex B in part D of this report.

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The table A.1 presented in Annex A of the Security Target [6] gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines the standard of application where its specific appropriateness is stated. *The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). An explicit validity period is not given.*

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 3 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, a Security Target Lite [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12. Regulation specific aspects (eIDAS, QES)

None.

13. Definitions

13.1. Acronyms

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
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
CVCA	Country Verifying Certificate Authority
DES	Data Encryption Standard
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
IC	Integrated Circuit
ICAO	International Civil Aviation Organisation
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
NVM	Non Volatile Memory
PACE	Password Authenticated Connection Establishment
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-1176-2023: “PWPW SmartApp-MRTD 1.0 Security Target”, Version 1.0.14.0, 2023-03-09, PWPW (confidential document)

Security Target Lite “PWPW SmartApp-MRTD 1.0 Security Target Lite”, Version 1.0.3.0, 2023-03-09, PWPW (public document)

[7] Evaluation Technical Report, Version 2, Date 2023-03-21, Evaluation Technical Report Summary BSI-DSZ-CC-1176, TÜV Informationstechnik GmbH (confidential document)

[8] Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE (EAC PP), Version 1.3.2, 5 December 2012, BSI-CC-PP-0056-V2-2012-MA-02,
Common Criteria Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE_PP), Version 1.01, 22 July 2014, BSI-CC-PP-0068-V2-2011-MA-01

[9] Certification Report – BSI-DSZ-CC-1110-V5-2022 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, 2022-04-29, Bundesamt für Sicherheit in der Informationstechnik.

Assurance Continuity Maintenance Report BSI-DSZ-CC-1110-V5-2022-MA-01 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, 2022-09-09, Bundesamt für Sicherheit in der Informationstechnik.

[10] “PWPW SmartApp-MRTD 1.0 Preparative procedures – pre-personalization”, Version 1.0.11.0, Date 2022-12-13, PWPW

[11] ETR for composite evaluation according to AIS 36 for the Product BSI-DSZ-CC-1110-V5-2022, v1, 2022-03-29, TÜV Informationstechnik GmbH.

[7] specifically

- 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 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 5, Kompositionsevaluierung including JIL Document and CC Supporting Document

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-1176-2023

Evaluation results regarding development and production environment

The IT product PWPW SmartApp-MRTD 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 Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 22 May 2023, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (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) PWPW SmartApp Development Site; Sanguszki 1 Street, 00-222 Warsaw, Poland; SW Development; Certification ID BSI-DSZ-CC-S-0168-2021-MA-01.

b) For development and production sites regarding the platform IC from Infineon Technologies AG, please refer to the certification report [9], Product Certificate (Initialization/Pre-personalization, IC Development, IC Manufacturing)

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