Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0985-2018

for

Machine Readable e-Document with „ICAO Application", Extended Access Control with PACE based on National Operating System (NOS) NOS e-Passport (EAC with PACE) v.1.01-I

from

Universal Information Technologies LLC

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-0985-2018 (*)

Security IC with MRTD EAC/PACE Application

Machine Readable e-Document with „ICAO Application", Extended Access Control with PACE based on National Operating System (NOS) NOS e-Passport (EAC with PACE) v.1.01-I

from	Universal Information Technologies LLC
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
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_DVS.2, ATE_DPT.2 and AVA_VAN.5

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 4

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria
Recognition Arrangement
recognition for components
up to EAL2

Bonn, 27 November 2018

For the Federal Office for Information Security

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

Bernd Kowalski
Head of Division

L.S.

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 BSIG1 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]
- BSI Schedule of 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 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

- 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.sogisportal.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: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the 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 Machine Readable e-Document with „ICAO Application", Extended Access Control with PACE based on National Operating System (NOS) NOS e-Passport (EAC with PACE) v.1.01-I has undergone the certification procedure at BSI.

The evaluation of the product Machine Readable e-Document with „ICAO Application", Extended Access Control with PACE based on National Operating System (NOS) NOS e-Passport (EAC with PACE) v.1.01-I was conducted by T-Systems International GmbH. The evaluation was completed on 5 November 2018. T-Systems International GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Universal Information Technologies LLC.

The product was developed by: Universal Information Technologies LLC.

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 27 November 2018 is valid until 26 November 2023. 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 Machine Readable e-Document with „ICAO Application", Extended Access Control with PACE based on National Operating System (NOS) NOS e-Passport (EAC with PACE) v.1.01-I 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] Universal Information Technologies LLC
Chervonoarmiyska Street, 55
03150 Kyiv
Ukraine

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 Machine Readable e-Document with „ICAO Application", Extended Access Control with PACE based on National Operating System (NOS) NOS e-Passport (EAC with PACE) v.1.01-I.

The TOE is a Machine Readable e-Document with „ICAO Application", Extended Access Control with PACE running on the microcontroller Infineon Security Controller M7892 B11 (BSI-DSZ-CC-0782-V3-2017) [14, 15] and hosting the ePassport application as required by the Protection Profile [8].

The TOE is based on the products National Operating System (NOS) and the Hardware platform Infineon Security Controller M7892 B11 (BSI-DSZ-CC-0782-V3-2017) [14, 15] and is extended by functionality regarding machine readable electronic documents with extended access control. The extended functionality is the e-Passport application running on the NOS. From the logical point of view the TOE comprises the complete product of its parts and is not restricted to any subset.

The TOE is an electronic document representing a contactless smart card programmed according to ICAO Technical Report "Supplemental Access Control" [11] (which means amongst others according to the Logical Data Structure (LDS) defined in [12]) and additionally providing the Extended Access Control according to the 'ICAO Doc 9303 [10] and BSI TR-03110 [13], respectively. The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to Electronic Passport using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2-2011 [9].

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

TOE Security Functionality	Addressed issue
TSS_Access_Control	The TOE provides access control mechanisms for restricting access to a set of objects stored in the TOE
TSS_Trusted_Channel	This TOE security service enforces establishment and operation of secure channels.
TSS_Authentication	This TOE security service enforces authentication procedures.
TSS_Self-Protection	The TOE enforces this TOE security service in

TOE Security Functionality	Addressed issue
	order to protect its own genuineness (TSF and TSF-data) and to support the protection of user data stored in the TOE.

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.

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:

Machine Readable e-Document with „ICAO Application", Extended Access Control with PACE based on National Operating System (NOS) NOS e-Passport (EAC with PACE) v.1.01-I

The TOE (ST BSI-DSZ-CC-0985) is a composite product and includes the certified hardware platform and Embedded Software.

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/SW	Infineon Security Controller M7892 B11 including the corresponding Infineon cryptographic libraries (BSI-DSZ-CC-0782-V3-2017)	-	Secure Delivery
		IC Embedded Software (National Operating System) and e-Passport application as binary file - hash value: b3 3a a3 cd 85 fa 01 83 07 97 8b d1 55 a5 55 02 de d6 25 21 b5 76 18 5b 93 7d a5 20 8c 2b f8 47	Date: 17.02.2017 Version: 1.01-I Build number: 0.33	Secure Delivery

No	Type	Identifier	Release	Form of Delivery
3	DOC	Operational User Guidance (AGD_OPE), Machine Readable e-Document with „ICAO Application", based on National Operating System (NOS), NOS e-Document (EAC with PACE) v.1.01-I, BSI_DCZ_CC-0985, Universal Information Technologies LLC, BSI_DCZ_CC-0985	version 1.2, 12.09.2017 [16]	Delivered in electronic form.
4	DOC	Preparative Procedures (AGD_PRE), Machine Readable e-Document with „ICAO Application", based on National Operating System (NOS), NOS e-Document (EAC with PACE) v.1.01-I (BSI_DCZ_CC-0985), NOS e-Document (BAC) v.1.01-I, Universal Information Technologies LLC (BSI_DCZ_CC-0987)	version 0.28, 13.11.2017 [17]	Delivered in electronic form.

Table 2: Deliverables of the TOE

The TOE includes the certified hardware platform and Embedded Software.

The delivery procedure starts at the integration and personalisation step. The party responsible for the composite product integration is called "product integrator" and is played by the State Enterprise "Polygraph Combine Ukraina". This organisation also performs the personalisation step in the role of "personalisation agent". The delivery destination (the "user") is the Ukrainian passport issuing authority.

The TOE as the final composite product is uniquely identified by the TOE's answer to command GET INFO (CLA = '80', INS = 'B0', P1 = '00', P2 = '00', Lc Field = '00' Data Field = 'absent', L2 Field = 'absent') as follows:

Data Field = '4e 4f 53 76 31 2e 30 31 2d 49 62 30 2e 33 33 64 31 37 30 32 32 30 31 37 68 b3 3a a3 cd 85 fa 01 83 07 97 8b d1 55 a5 55 02 de d6 25 21 b5 76 18 5b 93 7d a5 20 8c 2b f8 47'

In this context the TOE is identified by GET_INFO APDU command as follows:

- Embedded software version number: "1.01-I",
- Embedded software build number "0.33",
- Date of Embedded software building: "17.02.2017",
- Hash value: "b3 3a a3 cd 85 fa 01 83 07 97 8b d1 55 a5 55 02 de d6 25 21 b5 76 18 5b 93 7d a5 20 8c 2b f8 47".

The Embedded Software for the TOE is delivered from the Embedded Software Manufacturer to the Composite Product Integrator in a secure way.

The Embedded Software supporting documents [16 and 17] are delivered from the Embedded Software Manufacturer to the Composite Product Integrator in a secure way and marked as "National Operating System (EAC with PACE) v.1.01-I".

The IC (M7892 B11) as the Hardware Platform for the TOE is identified by its Chip Identification Data (see [14] and [15]). The Inlays are delivered from the IC Manufacturer to the Composite Product Integrator in the secure way only. For any data writing to IC M7892 B11 unique transport keys are used. The transport keys will be wrong for other types of IC.

3. Security Policy

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

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The list of objectives which have to be met by the the environment can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

The TOE referenced to is a contactless smartcard based on the products National Operating System (NOS) and the Hardware platform Infineon Security Controller M7892 B11 (BSI-DSZ-CC-0782-V3-2017) and is extended by functionality regarding machine readable electronic documents with extended access control. The extended functionality is the e-Passport application executed by the NOS.

The security functions of the TOE are:

- TSS_Access_Control
- TSS_Trusted_Channel
- TSS_Authentication
- TSS_Self-Protection

The TOE platform is given by the certified hardware platform Infineon Security Controller M7892 B11. This platform contains certified cryptographic libraries that provide corresponding interfaces to the platform user.

On top of this platform the TOE architecture defines dedicated subsystems that provide the TOE functionality: A protocol manager handles the communication between the TOE and the card terminal using contactless communication. A command dispatcher interacts with the protocol manager and is responsible for the identification of received commands and to build the corresponding response frames. A persistency subsystem is responsible for data writing, reading and storage using the underlying platform. This subsystem also provides the integrity of the stored data. The cryptographic subsystem provides an interface to the cryptographic features of the TOE. The requests are partly forwarded to the underlying platform and partly implemented in this subsystem. It provides access to random numbers, to hash values, digital signatures and performs cryptographic operations on the data. The

generation and destruction of cryptographic keys is also provided by the subsystem. A subsystem for identification and authentication is responsible for identification and authentication of external card terminals. Also, the card terminal can identify and authenticate the TOE using this subsystem. Another subsystem provides the trusted channel between the TOE and the card terminal and ensures the integrity, authenticity and confidentiality of the exchanged data.

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 Tests

The tests performed by the developer can be divided into the following categories:

- tests which are performed in a simulation environment with different tools for the analogue circuitries and for the digital parts of the TOE;
- functional tests which are performed with special software;
- characterisation and verification tests to release the hardware platform for production including tests with different operating conditions as well as special verification tests for security services and security features of the hardware;
- functional tests at the end of the production process using IC Dedicated Test Software. These tests are executed for every chip to check its correct functionality as last step of phase 3.

The developer tests cover all TSFIs as identified in the functional specification as well as in the test documentation.

Evaluator Tests

The evaluators were able to repeat the tests of the developer. A test protocol of the tests provided by the developer was verified. The tests of the developer are repeated by sampling. In addition the evaluators performed independent tests to supplement, augment and to verify the tests performed by the developer.

The evaluation provides evidence that the current version of the TOE provides the TOE Security Functionality as specified by the developer. The test results confirm the correct implementation of the TOE Security Functionality.

For penetration testing the evaluators took all TOE Security Functionality into consideration. Extensive penetration testing was performed to test the security mechanisms used to provide the Security Services and Security Features.

The evaluators performed the tests using smart cards with the software or using the emulator. For both cases, the correct software image was used. The SHA1 function cannot be called by the final product. Therefore the developer implemented additional command interface to call the function for SCA tests.

All tests were carried out in developer's environment with the test samples configured as the TOE, except for the SHA1-SCA tests. By the tests carried out using the emulators, the same device image was loaded as the TOE.

For the side channel analysis of the SHA1 function the evaluators used the test samples provided for the SHA1 side channel analysis. For this purpose the developer provided two kind of test samples:

- Test samples configured as intended TOE
- Test samples with additional command interface for SHA1 function

Reading the value provided by the TOE, the evaluators verified the test samples provided by the developer using GET_INFO command.

Having read the information the evaluators verified that the information read from the tests samples were same as depicted in section 1.2 of the Security Target [6], except for the "checksum", that is hash value for embedded software based on SHA-256 provided by the test samples with additional command interface for SHA1 function. Considering the embedded software of those test samples included additional command interfaces, this was according to the expectation of the evaluators.

The evaluators documented the tested configurations and the validity of test results for the TOE.

Considering the potential vulnerability of the SHA1 function, the evaluator received test samples that were configured exactly as the TOE. The evaluators verified the configuration by reading the SHA256-HASH value, that was identical to the hash value shown in section 1.2 of the Security Target [6], with the GET_INFO command. However the TOE does not allow to call the SHA1 function directly. Therefore the effort for a side channel analysis would be increased significantly by collecting the signal tracks and by the analysis. Accordingly the evaluators used additional test samples with direct interface to the SHA1 function.

The tests showed that the TOE works as expected and no vulnerabilities were identified.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

The TOE (BSI-DSZ-CC-0985) is identified by GET_INFO APDU command as follows:

- Embedded software version number: "1.01-I",
- Embedded software build number "0.33",
- Date of Embedded software building: "17.02.2017",
- Hash value:
  "b3 3a a3 cd 85 fa 01 83 07 97 8b d1 55 a5 55 02 de d6 25 21 b5 76 18 5b 93 7d a5 20 8c 2b f8 47".
  (For details please see the Security Target [6], chapter 1.2.)

The TOE is a composite product. The TOE includes the certified hardware platform and Embedded Software.

The IC (M7892 B11) as the Hardware Platform for the TOE is identified by its Chip Identification Data (see [14] and [15]). The Inlays are delivered from the IC Manufacturer to

the Composite Product Integrator in the secure way only. For any data writing to IC M7892 B11 unique transport keys are used. The transport keys will be wrong for other types of IC.

The TOE as the final composite product is uniquely identified by the TOE's answer to command GET INFO (CLA = '80', INS = 'B0', P1 = '00', P2 = '00', Lc Field = '00' Data Field = 'absent', L2 Field = 'absent') as follows:

Data Field = '4e 4f 53 76 31 2e 30 31 2d 49 62 30 2e 33 33 64 31 37 30 32 32 30 31 37 68 b3 3a a3 cd 85 fa 01 83 07 97 8b d1 55 a5 55 02 de d6 25 21 b5 76 18 5b 93 7d a5 20 8c 2b f8 47'

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:

- Application of CC to Integrated Circuits,
- Attack Methods for Smartcards and Similar Devices,
- Application of Attack Potential to Smartcards,
- Evaluation Methodology for CC Assurance Classes for EAL5+ and EAL6,
- Composite product evaluation for Smart Cards and similar devices (see AIS 36). According to this concept the relevant guidance documents of the underlying platform and the documents ETR for Composition from the platform evaluations (i.e. on hardware) have been applied in the TOE evaluation.

(see [4], AIS 25, 26, 34, 46).

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

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

All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)

- The components ALC_DVS.2, ATE_DPT.2 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 [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, ATE_DPT.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 following table 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.

Purpose	Cryptographic Mechanism	Standard of Implementation [18]	Key Size in Bits	Standard of Application [18]	Comment
Authenticity	ECDSA-signature verification of card verifiable certificates using SHA-256	ISO/IEC 15946-2-2002, Part 2 (ECDSA) FIPS PUB 180-4 (SHA)	|k|=256 Elliptic curve BrainpoolP256r1 (RFC 5639)	ICAO 9303, Part 11	FCS_COP.1/ SIG_VER, see [6], section 6.1.3
Authentication	PACE	TR-03110-1, v.2.20 (PACEv2)	|Nonce|=128 MRZ=88 bytes, keying material=24 CAN=6 bytes, CAN itself is keying material	ICAO-TR SAC, v.1.01 TR-03110-1, v.2.20 (MRZ, CAN)	FIA_UAU.1/ PACE, FIA_UAU.5/ PACE, FIA_UAU.6/ PACE, FIA_AFL.1/ PACE, see [6], section 6.1.3
	Chip Authentication v.1 for authentication of travel document's chip to inspection system based on ephemeral-static ECDH in combination with 3DES	TR-03111, v.2.0 (ECDH) ANS X9.52 (3DES)	|k|=112 Elliptic curve BrainpoolP256r1 (RFC 5639)	ICAO 9303, Part 11 TR-03110-1, v.2.20	FIA_API.1, FIA_UAU.5/ PACE, FIA_UAU.6/ EAC, see [6], section 6.1.3
	Terminal Authentication v.1 for authentication of inspection system to travel document's chip based on ECDSA using SHA-256	ISO/IEC 15946-2-2002, Part 2 (ECDSA) FIPS PUB 180-4 (SHA)	|k|=256 Elliptic curve BrainpoolP256r1 (RFC 5639)	ICAO 9303, Part 11 TR-03110-1, v.2.20	FIA_UAU.1/ PACE, FIA_UAU.5/ PACE see [6], section 6.1.3
Key Agreement	ECDH using	TR-03111, v.2.0	|k|=256	ICAO-TR SAC,	FCS_CKM.1/

Purpose	Cryptographic Mechanism	Standard of Implementation [18]	Key Size in Bits	Standard of Application [18]	Comment
	SHA-1	(ECDH) FIPS PUB 180-4 (SHA) ICAO-TR SAC, v.1.01	Elliptic curve BrainpoolP256r1 (RFC 5639)	v.1.01 TR-03110-1, v.2.20	DH_PACE
Confidentiality	3DES in CBC mode	ANS X9.52 (3DES) SP 800-38A (CBC) ICAO 9303, Vol. 2, Appendix 5, A5.3	|k|=112	ICAO 9303, Part 11 ICAO-TR SAC, v.1.01	FCS_COP.1/ PACE_ENC
Integrity	3DES in Retail MAC mode	FIPS PUB 46-3 (DES) ANS X9.52 (3DES) ISO/IEC 9797-1:2011 (Retail MAC)	|k|=112	ICAO 9303, Part 11 ICAO-TR SAC, v.1.01	FCS_COP.1/ PACE_MAC
Trusted Channel	Secure messaging in ENC_MAC mode is established during PACE	TR-03110-1, v.2.20 (PACE), additionally cf. entries 2, 5-7		ICAO 9303, Part 11 TR-03110-1, v.2.20	FTP_ITC.1/ PACE
	Secure messaging in ENC_MAC mode is established during Chip Authentication v1 after PACE	TR-03110-1, v.2.20, additionally cf. entries 2, 3, 5-7		ICAO 9303, Part 11 TR-03110-1, v.2.20	FTP_ITC.1/ PACE, FCS_CKM.1/ CA
Cryptographic primitive	Deterministic RNG DRG.3	Compliance to AIS20/31	n.a.	TR-03116-2 (DRG-3)	Provided by the underlying certified platform (FCS_RNG.1)

Table 3: TOE cryptographic functionality

Note: The Standards of Implementation and Application are referenced in [18].

The strength of the these cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2).

All cryptographic algorithms listed here are implemented by the TOE because of the standards building the TOE application. For that reason, an explicit validity period is not given for this crypto functionality.

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Definitions

12.1. Acronyms

AA	Active Authentication
AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
APDU	Application Protocol Data Unit
BAC	Basic Access Control
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CA	Chip Authentication
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
DES	Data Encryption Standard; symmetric block cipher algorithm
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ETR	Evaluation Technical Report
ICAO	International Civil Aviation Organisation
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LDS	Logical Data Structure

MAC	Message Authentication Code
MRTD	Machine Readable Travel Document
NOS	National Operating System
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
RNG	Random Number Generator
SAR	Security Assurance Requirement
SCA	Side Channel Analysis
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SM	Secure Messaging
ST	Security Target
TA	Terminal Authentication
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2. Glossary

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

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

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

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

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

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

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

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

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, April 2012
Part 2: Security functional components, Revision 4, April 2012
Part 3: Security assurance components, Revision 4, April 2012
http://www.commoncriteriaportal.org

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

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

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[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-0985-2018, 'Machine Readable e-Document with „ICAO Application", Extended Access Control with PACE based on National Operating System (NOS), NOS e-Passport (EAC with PACE) v.1.0-I', Version 1.0 Date 31.08.2018, Universal Information Technologies LLC

[7] Evaluation Technical Report BSI-DSZ-CC-0985-2018, Machine Readable Electronic Document with ICAO Application, Extended Access Control with PACE based on National Operating System (NOS), NOS e-Passport (EAC with PACE) v.1.01-I, Version 1.2, Date 30.10.2018, T-Systems International 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

[9] BSI-CC-PP-0068-V2-2011, Common Criteria Protection Profile / Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), BSI, Version 1.0, 02.11.2011

[7] specifically

- AIS 25, Version 7, Anwendung der CC auf Integrierte Schaltungen
- AIS 26, Version 10, Evaluations Methodologie für in Hardware Integrierte Schaltungen
- 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 36, Version 4, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.9, Reuse of evaluation results

[10] ICAO Doc 9303-1, Specifications for electronically enabled passports with biometric identification capabilities. In Machine Readable Travel Documents – Part 1: Machine Readable Passport, volume 2, ICAO, 6th edition, 2006

[11] ICAO TR-SAC, MACHINE READABLE TRAVEL DOCUMENTS, TECHNICAL REPORT: Supplemental Access Control for Machine Readable Travel Documents, Version 1.00, November 2010

[12] ICAO TR-LDS, MACHINE READABLE TRAVEL DOCUMENTS, Technical Report: Development of a Logical Data Structure - LDS - for optional Capacity Expansion Technologies, May 2004

[13] TR-03110-1, Technical Guideline: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.20, 26.02.2015, Bundesamt für Sicherheit in der Informationstechnik (BSI)

[14] Security Target BSI-DSZ-CC-0782-V3-2017, Version 2.6, 2017-08-02, Security Target Lite M7892 B11

[15] Certification Report BSI-DSZ-CC-0782-V3-2017 for Infineon Security Controller M7892 B11 from Infineon Technologies AG, Bundesamt für Sicherheit in der Informationstechnik, 05.09.2017

[16] Operational User Guidance (AGD_OPE), Machine Readable e-Document with „ICAO Application", based on National Operating System (NOS), NOS e-Document (EAC with PACE) v.1.01-I, BSI_DCZ_CC-0985, Universal Information Technologies LLC, BSI_DCZ_CC-0985, version 1.2, 12.09.2017

[17] Preparative Procedures (AGD_PRE), Machine Readable e-Document with „ICAO Application", based on National Operating System (NOS), NOS e-Document (EAC with PACE) v.1.01-I (BSI_DCZ_CC-0985), NOS e-Document (BAC) v.1.01-I, Universal Information Technologies LLC (BSI_DCZ_CC-0987), version 0.28, 13.11.2017

[18] - **ANS X9.52**: AMERICAN NATIONAL STANDARD FOR FINANCIAL SERVICES - TRIPLE DATA ENCRYPTION ALGORITHM MODES OF OPERATION. 29.7.1998
- **FIPS PUB 180-4**: Secure Hash Signature Standard (SHS). NIST, March 2012
- **FIPS PUB 46-3**: DATA ENCRYPTION STANDARD (DES). NIST. 25.10.1999
- **ICAO-TR SAC**: MACHINE READABLE TRAVEL DOCUMENTS. TECHNICAL REPORT. Supplemental Access Control for Machine Readable Travel Documents. Version 1.01, 11.11.2010. ISO/IEC JTC1 SC17 WG3/TF5 FOR THE INTERNATIONAL CIVIL AVIATION ORGANIZATION.
- **ISO/IEC 15946-2-2002**: Information technology - Security techniques - Cryptographic techniques based on elliptic curves - Part 2: Digital signatures. Edition 1, December 2002
- **ICAO 9303**: Machine Readable Travel Documents. Part 2 - Specifications for the Security of the Design, Manufacture and Issuance of MRTDs. Edition 7, 2015.
- **ISO/IEC 9797-1**: Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher. Edition 2, March 2011
- **SP 800-38A**: NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques: December 2001
- **TR-03110-1**: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token - Part 1 - eMRTDs with BAC/PACEv2 and EACv1,

Version 2.20, 26.2.2015, BSI
- **TR-03111**: Technical Guideline TR-03111: Elliptic Curve Cryptography, Version 2.0, 28.6.2012, BSI

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 10.4
- 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 11
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 12 to 16
- 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 http://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-0985-2018

Evaluation results regarding development and production environment

The IT product Machine Readable e-Document with „ICAO Application", Extended Access Control with PACE based on National Operating System (NOS) NOS e-Passport (EAC with PACE) v.1.01-I (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 and 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 27 November 2018, 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, and ALC_TAT.1)

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

a) SW development and test site ("UniTech"): Universal Information Technologies LLC, 55 Chervonoarmiyska Str. ,Kyiv, 03150, Ukraine

b) Integration/Production/Persoalisation site ("PCU"): Polygraph Combine "Ukraina", 38-44 Dehtiarivska Str., Kyiv, 04119, Ukraine

c) For development and production sites regarding the platform please refer to the certification reports BSI-DSZ-CC-0782-V3-2017 for Infineon Security Controller M7892 B11 from Infineon Technologies AG [15]

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6]) are fulfilled by the procedures of these sites.

Note: End of report