Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1090-2018

for

Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application“, Extended Access Control with PACE

from

cv cryptovision GmbH

sponsored by

Veridos GmbH - Identity Solutions by G+D BDR

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-1090-2018 (*)

Security IC with MRTD EAC/PACE Application

Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application“, Extended Access Control with PACE

from	cv cryptovision GmbH
sponsored by	Veridos GmbH - Identity Solutions by G+D BDR
PP Conformance:	Common Criteria 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, 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 5 augmented by ALC_DVS.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.

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

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, 18 December 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 licensing 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: https://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

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

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

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application“, Extended Access Control with PACE has undergone the certification procedure at BSI.

The evaluation of the product Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application“, Extended Access Control with PACE was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 14 December 2018. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Veridos GmbH - Identity Solutions by G+D BDR.

The product was developed by: cv cryptovision GmbH.

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

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 18 December 2018 is valid until 17 December 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 Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application“, Extended Access Control with PACE 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] cv cryptovision GmbH
Munscheidstr. 14
45886 Gelsenkirchen
Deutschland

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The composite TOE is named “Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE” and short named “ePasslet3.0/MRTD-EAC”. It consists of an applet configuration “ePasslet3.0/MRTD-EAC” provided by the Veridos Suite v3.0 – cryptovision ePasslet Suite used for electronic travel documents providing EAC (Extended Access Control) with PACE (Password Authenticated Connection Establishment), the according guidance documents [11], [12] and [13], the underlying operating system and the hardware platform with the crypto library. There is only one certified configuration of the TOE.

The platform comprises of the certified integrated circuit Infineon M5073 G11 [14] (certificate ID BSI-DSZ-CC-0951-2015-RA-01) and the certified Java Card operating system SmartCafé Expert 7.0 C3 [15] (certificate ID BSI-DSZ-CC-1028-2017-MA-01) including the crypto library of the Java Card OS platform by G+D. The IC provides an interface for contact-based communication and hardware for contactless communication.

The MRTD contains physically visible data including but not limited to personal data of the holder as, biographical data, the printed data in the MRZ (Machine Readable Zone) and the printed portrait. Further, the MRTD contains digital personal data of the MRTD holder, i.e. the digital MRZ, the digitized portrait, the biometric reference of fingers or iris images, the document security object and other data according to the LDS (Logical Data Structure).

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

- Common Criteria 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] and
- 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]

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 5 augmented by 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 6.2. 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
TSF_Access	Access Control
TSF_Admin	Administration
TSF_Secret	Secret key management
TSF_Crypto	Cryptographic operations

TOE Security Functionality	Addressed issue
TSF_SecureMessaging	Secure Messaging
TSF_Auth	Authentication protocols
TSF_Integrity	Integrity protection
TSF_OS	Java Card OS Security Functionalities

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 6.2.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.2, 3.3 and 3.4.

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:

Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application“, Extended Access Control with PACE

As the TOE is an application on top of a composite TOE (certified Java Card OS) there are deliveries from the application developer to the OS manufacturer (Table 2) and deliveries to the customer (Table 3).

The following table outlines the TOE deliverables to the OS developer (G+D):

No	Type	Identifier	Release	Form of Delivery
1.	SW	Veridos Suite v3.0 – cryptovision ePasslet Suite	3.0	Delivery from cryptovision (developer) to G+D (manufacturer): The applet and the guidance documents are delivered by encrypted e-mail. Thereby the PGP/GPG encryption with an at least 2048 bit asymmetric key and AES 256 is used to
2.	DOC	Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing an ICAO MRTD application with Extended Access Control (EACv1) or with Basic Access Control (BAC) and Supplemental Access Control (SAC) Operational Guidance (AGD_OPE) [12]	3.0.5	
3.	DOC	Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card Applet Suite providing Electronic ID Documents applications Guidance Manual [11]	3.0.11	

No	Type	Identifier	Release	Form of Delivery
4.	DOC	Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing an ICAO MRTD application with Extended Access Control (EACv1) or with Basic Access Control (BAC) and Supplemental Access Control (SAC) Preparation Guidance (AGD_PRE) [13]	3.0.12	preserve confidentiality and integrity.

Table 2: TOE Deliverables from application developer to OS developer

In addition to the above mentioned methods of delivery and the according security mechanism, the correctness of delivery is proven with a hash over the received decrypted applet, which is sent back to the developer. The developer then compares the received hash value with the hash value of the delivered applet. Furthermore, samples are provided by the manufacturer to the developer for functional testing to verify the correct functionality of the composite TOE.

The following TOE deliverables are provided to the customer:

No	Type	Identifier	Release	Form of Delivery
1.	HW+SW	Veridos eDoc Suite v3.0 – cryptovision ePasslet Suite on platform SmartCafé Expert 7.0 C3	3.0	The delivery process is included in the evaluation of the underlying smartcard OS. The TOE is already protected by the OS. The delivery is performed with sealed boxes by courier.
2.	DOC	Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing an ICAO MRTD application with Extended Access Control (EACv1) or with Basic Access Control (BAC) and Supplemental Access Control (SAC) Operational Guidance (AGD_OPE) [12]	3.0.5	The delivery process is included in the evaluation of the underlying smartcard OS. Signed and encrypted Email delivery using PGP RSA 2048bit is used.
3.	DOC	Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card Applet Suite providing Electronic ID Documents applications Guidance Manual [11]	3.0.11	
4.	DOC	Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing an ICAO MRTD application with Extended Access Control (EACv1) or with Basic Access Control (BAC) and Supplemental Access Control (SAC) Preparation Guidance (AGD_PRE) [13]	3.0.12	
5.	DOC	Preparative Procedures Sm@rtCafé® Expert 7.0 C3 [16]	3.6	
6.	DOC	Operational User Guidance Sm@rtCafé® Expert 7.0 C3 [17]	5.2	

Table 3: TOE deliverables to the customer

The TOE can be identified in accordance with the described processes in [6] and [13], chapter 2.5.3. After the delivery the TOE can be identified by the command response sequence as outlined in the Security Target [6], chapter 1.3.2.1 and [13], chapter 2.5.3,

verifying the configuration and the life cycle of the underlying platform OS, as well as the CPLC-Data.

After instantiation of the applet it can be selected and the version of the applet can be verified, as well as the internal version number, see [13], chapter 2.5.3.

The composite TOE consists of the underlying hardware platform, the SmartCafé Expert 7.0 C3 operating system including the crypto library and the Veridos eDoc Suite v3.0 – cryptovision ePasslet Suite in applet configuration “ePasslet3.0/MRTD-EAC”. First, the generated applet suite and the guidance are delivered by encrypted e-mail from the development to the production site. Either the SmartCafé Expert operating system with the applet is integrated into the ordered IC by the IC manufacturer, or the smartcard embedded software developer, here G+D, loads the SW part with the flash loader. Afterwards the composite TOE is delivered in the sense of Common Criteria. Thereby the delivery process is the same for the composite product as the delivery process covered by the certified SmartCafé Expert 7.0 C3 composite TOE. The guidance documents [17] and [18] of the platform outline the delivery procedure. The product is delivered within sealed boxes by courier and is additionally secured by the operating system security mechanisms. The TOE guidance is delivered in electronic form (encrypted and signed) according to defined mailing procedures by G+D. The delivery in sense of CC is fully covered by the underlying platform certification of the SmartCafé Expert 7.0 C3.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Security Audit,
- Cryptographic Support,
- User Data Protection,
- Identification and Authentication,
- Security Management,
- Protection of the TOE Security Functions and
- Trusted Path / Channels.

Specific details concerning the above mentioned security policies can be found in Chapter 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 and measures to be taken by the IT environment, the user or the risk manager. The following topics are of relevance and considered in [13], chapter 2.4:

- OE.Auth_Key_Travel_Document,
- OE.Authoriz_Sens_Data,
- OE.Exam_Travel_Document,

- OE.Prot_Logical_Travel_Document,
- OE.Ext_Insp_System,
- OE.Active_Auth_Key_MRTD,
- OE.Legislative_Compliance,
- OE.Passive_Auth_Sign,
- OE.Personalisation,
- OE.Terminal,
- OE.Travel_Document_Holder,
- OE.APPLET,
- OE.VERIFICATION, and
- OE.CODE_EVIDENCE

5. Architectural Information

The composite TOE, Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE, is a Java Card applet based on a certified Java Card platform comprising eight subsystems, listed with a short description in the following itemization:

- Platform: Represents the parts of the underlying hardware platform of the composite TOE, which interacts with the application in regards of control, including the creation and selection of applet instance and the internal life cycle control.
- Operating System: Represents the operating system of the underlying G+D platform of the composite TOE, which is used by the applications to realize the functionality. It also comprises the underlying cryptographic library.
- Configuration Manager: Provides services for applet creation and configuration. This subsystem is called by the platform subsystem each time an application is instantiated.
- Event Manager: Handles events from internal subsystems and from the underlying platform and calls other subsystems interfaces to process these events.
- Command Processor: Provides the main interface to the platform by passing through APDU commands from the terminal to the applet. The subsystem decides if special APDUs have to be handled by the application and ensures their execution by the responsible applet. It also provides access controlled execution of commands covering all applet commands.
- Secure Messaging Manager: Handles the secure channel between the application and the terminal in accordance with the specified cryptographic mechanisms and key sizes. The responsibility for secure messaging includes the verification of MAC, unwrapping messages and security mechanisms for secure messaging.
- File System Manager: Provides an interface for file and object access and management by a representation of the existing elements.

- State Manager: Handles the internal state of the application and provides update functionality and access to the current DF, EF, KO, security environment, and the authentication status of the terminal and the challenge.

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

The tests were performed with the composite smartcard product “ePasslet3.0/MRTD-EAC” on G+D OS SmartCafé Expert 7.0 C3, in the one configuration in scope of the certification.

Developer’s testing approach:

The developer considered the following aspects when designing his test approach:

- Tests to cover all actions defined in [19],
- Good case and bad case tests for each command defined in the document [19] and executable on the TOE,
- Access rules tests as part of the requirements on TSF data,
- Tests covering all TSF subsystems in the TOE design.

Test results:

All test cases in each test suite were run successfully on this TOE version. The developer’s testing results demonstrate that the TOE operates as expected.

Evaluator’s testing approach:

The TOE consists of the Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application”, Extended Access Control with PACE installed on SmartCafé Expert 7.0 C3 OS. The APDU tests were performed using standard PC Smartcard readers, a standard PC, test software provided by the developer as well as evaluator’s test software. Further, for some tests, i.e. fuzzing, B0 card readers (supporting also raw communication) were used. The choice of the subset of interfaces used for testing has been done according to the following approach:

- Augmentation of developer testing for interfaces and supplementation of developer testing strategy for interfaces are both used for setting up test cases.
- Besides augmentation and supplementation of developer’s tests the tests are also selected by the complexity and the susceptibility to vulnerabilities of interfaces and related functionality.
- Since the developer has tested all interfaces and the rigour of developer testing of the interfaces is sufficient, the evaluator found that all TSFIs have been suitably tested. The evaluator had no doubt that an interface is not properly implemented.
- The APDU interfaces are essential for the TOE and therefore in the focus of testing.

- Implicit testing was sufficiently included in developer testing because preparative steps were performed and described for nearly each test case.
- The selection process is based on evaluation experience of the evaluation body. Therefore, all TOE security functionality is included within the subset. Nearly all cryptographic functionality is provided by the platform and was sufficiently tested during platform evaluation. Cryptographic functionalities implemented in the applet suite were tested in the current evaluation.

Test results:

The test prerequisites, test steps, and expected results adequately test the related TSFI, and they are consistent with the descriptions of the TSFI in the functional specification. The test results have not shown any deviations between the expected test results and the actual test results.

The penetration testing was performed at the site of the evaluation body TÜViT in the evaluator's test environment with the evaluator's test equipment. The samples were provided by the sponsor and by the developer. The test samples were configured and parametrized 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 the attack potential high was actually successful in the TOE's operational environment as defined in [6] provided that all measures required by the developer are applied.

8. Evaluated Configuration

There is only one configuration of the TOE, as described in section 1 above. For all tests the TOE is configured and parametrised, if necessary, according to the guidance documents. The "ePasslet 3.0/MRTD-EAC" TOE configuration is generated out of the applet suite and loaded in the underlying certified OS platform SmartCafé Expert 7.0 C3. The "ePasslet3.0/MRTD-EAC" applet needs to be created according to the guidelines given in [11] and [13].

9. Results of the Evaluation

9.1. CC specific results

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

The Evaluation Methodology CEM [2] was used for those components up to 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:

- *AIS 1, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers, Version 14, 11 October 2017*
- *AIS 14, Anforderungen an Aufbau und Inhalt der ETR-Teile (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 7, 03 August 2010,*

- *AIS 19, Anforderungen an Aufbau und Inhalt der Zusammenfassung des ETR (Evaluation Technical Report) für Evaluationen nach CC (Common Criteria), Version 9, 03 November 2014,*
- *AIS 25, Anwendungen der CC auf integrierte Schaltungen, Version 9, 15 March 2017,*
- *AIS 26, Evaluationsmethodologie für in Hardware integrierte Schaltungen, Version 10, 03 July 2017,*
- *Special Attack Methods for Smartcards and Similar Devices, Version 1.4, 08 June 2011,*
- *AIS 34, Evaluation Methodology for CC Assurance Classes for EAL5+ (CC v2.3 & v3.1) and EAL6 (CC v3.1), Version 3, 03 September 2009,*
- *AIS 36, Kompositionsevaluierung, Version 5, 15 March 2017,*
- *AIS 37, Terminologie und Vorbereitung von Smartcard-Evaluierungen, Version 3, 17 May 2010,*

(see [4], AIS 26, 34, 36).

Additionally the CC Supporting Mandatory Technical Documents

- *Joint Interpretation Library – Composite product evaluation for Smart Cards and similar devices, Version 1.5.1, May 2018,*
- *Joint Interpretation Library – ETR template for composite evaluation of Smart Cards and similar devices, Version 1.1, August 2015 and*
- *Joint Interpretation Library – Minimum Site Security Requirements, Version 2.1 (for trial use), December 2017*

are considered.

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. [15, 16, 17, 18]), have been applied in the TOE evaluation.

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

- All components of the EAL 5 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_DVS.2 and AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Common Criteria 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],

  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]

- for the Functionality: PP conformant plus product specific extensions
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 5 augmented by 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.

The evaluation was performed as a composite evaluation according to AIS 36 and therefore relies on the platform certifications of the used IC (certification ID BSI-DSZ-CC-0951-2015) [20], [21]. This certified basis was used for SmartCafé Expert 7.0 C3 (certification ID BSI-DSZ-CC-1028-2017) [22] Composite TOE with an ETR for Composite Evaluation [23]. The RSA key generation was evaluated in the course of the evaluation of the crypto library of the Java Card OS by G+D. The platform IC underwent a Re-Assessment (certification ID BSI-DSZ-CC-0951-2015-RA-01) [14]. For a transparent incorporation of updated site certificates in the SmartCafé Expert 7.0 C3 software platform a maintenance procedure resulted in BSI-DSZ-CC-1028-2017-MA-01 [15]. This maintenance was related to ALC only, so the assurance statement of BSI-DSZ-CC-1028-2017 for the unchanged TOE remains valid. For compositions atop that composite TOE an ETR for Composite Evaluation addendum was provided [24].

9.2. Results of cryptographic assessment

The table in annex C in part D of this report presents 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 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 in the table in annex C in part D of this report 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 cryptographic functionality.

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in Table 2 and 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.

In addition, the following aspects need to be fulfilled when using the TOE:

- All requirements and recommendations in the guidance documentation [11], [12] and [13] shall be followed.

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

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
CPLC	Card Production Life Cycle
cPP	Collaborative Protection Profile
DF	Dedicated File
DES	Data Encryption Standard; symmetric block cipher algorithm
EAC	Extended Access Control
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
EF	Elementary File
ETR	Evaluation Technical Report
ICAO	International Civil Aviation Organisation
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
KO	Key Object
MAC	Message Authentication Code
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy

SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SM	Secure Messaging
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TÜViT	TÜV Informationstechnik GmbH

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 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-1090, Version 1.2, 06 December 2018, Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE, cv cryptovision GmbH

[7] Evaluation Technical Report BSI-DSZ-CC-1090, Version 1, 11 December 2018, TÜV Informationstechnik GmbH (confidential document)

[8] Common Criteria 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

[9] 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

[10] Configuration List for the TOE BSI-DSZ-CC-1090, 06 December 2018, 1090_1091_MRTD_conflist-SCE.XLSX, cryptovision GmbH (confidential document)

[11] Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card Applet Suite providing Electronic ID Documents applications Guidance Manual, Version 3.0.11, 06 December 2018, cryptovision GmbH

[12] Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing an ICAO MRTD application with Extended Access Control (EACv1) or with Basic Access Control (BAC) and Supplemental Access Control (SAC) Operational Guidance (AGD_OPE), Version 3.0.5, 06 December 2018, cryptovision GmbH

[13] Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing an ICAO MRTD application with Extended Access Control (EACv1) or with Basic Access Control (BAC) and Supplemental Access Control (SAC) Preparation Guidance (AGD_PRE), Version 3.0.12, 06 December 2018, cryptovision GmbH

[14] Assurance Continuity Reassessment Report, BSI-DSZ-CC-0951-2015-RA-01, Infineon Security Controller M5073 G11 with optional RSA2048/4096 v2.03.008, EC

[7] specifically

- AIS 1, Version 14, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 26, Version 10, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document

v2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG, 31 May 2017, Bundesamt für Sicherheit in der Informationstechnik

[15] Assurance Continuity Maintenance Report BSI-DSZ-CC-1028-2017-MA-01 SmartCafé Expert 7.0 C3 from Giesecke+Devrient Mobile Security GmbH, 04 October 2018, Bundesamt für Sicherheit in der Informationstechnik

[16] Preparative Procedures SmartCafé Expert 7.0 C3, Version 3.6, 10 August 2017, Giesecke+Devrient GmbH

[17] Operational User Guidance SmartCafé Expert 7.0 C3, Version 5.2, 07 August 2017, Giesecke+Devrient GmbH

[18] Security Target SmartCafé Expert 7.0 C3, Version 2.9, 16 August 2017, Giesecke+Devrient GmbH

[19] Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing an ICAO MRTD application with Extended Access Control (EACv1) or with Basic Access Control (BAC) and Supplemental Access Control (SAC) Functional Specification ADV_FSP, Version 3.0.1, 12 June 2018, cryptovision GmbH

[20] Certification Report – BSI-DSZ-CC-0951-2015 for Infineon Security Controller M5073 G11 with optional RSA2048/4096 v2.03.008, EC v2.03.008, SHA-2 v1.01 and Toolbox v2.03.008 libraries and with specific IC dedicated software (firmware) from Infineon Technologies AG, 11 November 2015, Bundesamt für Sicherheit in der Informationstechnik

[21] ETR FOR COMPOSITE EVALUATION (ETR-COMP), M5073 G11, BSI-DSZ-CC-0951, Version 4, 18 May 2017, TÜV Informationstechnik GmbH

[22] Certification Report BSI-DSZ-CC-1028-2017 for SmartCafé Expert 7.0 C3 from Veridos GmbH – Identity Solutions by G+D BDR, 08 September 2017, Bundesamt für Sicherheit in der Informationstechnik

[23] Evaluation Technical Report for Composite Evaluation according to AIS 36 for SmartCafé Expert 7.0 C3, Version 3, 16 August 2017, BSI-DSZ-CC-1028-2017, TÜV Informationstechnik GmbH

[24] Evaluation Technical Report for Composite Evaluation Addendum for SmartCafé Expert 7.0 C3, Version 1, 18 July 2018, BSI-DSZ-CC-1028-2017-MA-01, TÜV Informationstechnik GmbH

C. Excerpts from the Criteria

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

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailled 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 C: Overview of cryptographic functionalities implemented in the TOE

Annex B of Certification Report BSI-DSZ-CC-1090-2018

Evaluation results regarding development and production environment

The IT product Veridos Suite v3.0 – cryptovision ePasslet Suite – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application“, Extended Access Control with PACE (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 18 December 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.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2 and ALC_COMP.1) are fulfilled for the development and production sites of the TOE listed below:

a) cv cryptovision GmbH, Munscheidstr. 14, 45886 Gelsenkirchen, Germany, Software Development

b) The development and production sites of the underlying software platform are listed in [15]

c) The development and production sites of the underlying security IC platform are listed in [20]

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.

Annex C of Certification Report BSI-DSZ-CC-1090-2018

Overview of cryptographic functionalities implemented in the TOE

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Evaluator's Comments
1	Authenticity	ECDSA-signature verification of card verifiable certificates using SHA-{1,224,256, 384, 512}	[TR-03111] (ECDSA), [FIPS180-4] (SHA)	160, 192, 224, 256, 320, 384, 512, 521 bit; elliptic curves brainpoolP{160, 192, 224, 256, 320, 384, 512}r1, brainpoolP{160, 192, 224, 256, 320, 384, 512}t1 [Brainpool], secp P-{160, 192, 224, 256, 384, 521}r1 [SEC2]	[ICAODoc] (ECDSA), [TR-03110-1]	Verification of certificates for authentication. The cryptographic function is provided by the Java Card OS platform. (FCS_COP.1.1/ECDS A-VERI, FCS_COP.1.1/HASH)
2		RSASSA-PSS signature verification of card verifiable certificates using SHA-{1,224,256, 384, 512}	[RFC4056] (RSASSA-PSS), [FIPS180-4] (SHA)	Moduluslength = 512 - 2048 bit	[ICAODoc] (RSA), [TR-03110-1]	Verification of certificates for authentication. The cryptographic function is provided by the Java Card OS platform. (FCS_COP.1.1/RSA_ VERI, FCS_COP.1.1/HASH)
3	Authenticati on	PACE with SHA-1 or SHA-256	[ICAO_SAC]	Length of MRZ or CAN, |Nonce|=128	[ICAO-SAC], [TR-03110-1]	The basic cryptographic function is provided by the Java Card OS platform cf. FCS_CKM.1.1/ECC and according footnote (GDKeyAgreement), see [Platform-ST- lite, 8.1.1.2] The protocol itself is implemented in the applet.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Evaluator's Comments
4		Chip Authentication v.1 for authentication of travel document's chip to inspection system based on ephemeral-static ECDH in combination with AES	[ISO 15946] AES cf. Confidentiality/Integrity	160, 192, 224, 256, 320, 384, 512, 521 bit; elliptic curves brainpoolP{160, 192, 224, 256, 320, 384, 512}r1, brainpoolP{160, 192, 224, 256, 320, 384, 512}t1 [Brainpool], secp P-{160, 192, 224, 256, 384, 521}r1 [SEC2]	[ICAODoc], [TR-03110-1]	The basic cryptographic function is provided by the Java Card OS platform. The protocol itself is implemented in the applet. (FCS_CKM.1.1/ECC)
5		Chip Authentication v.1 for authentication of travel document's chip to inspection system based on ephemeral-static DH in combination with AES	[PKCS3], AES cf. Confidentiality/Integrity	Plength = 1024, 2048	[ICAODoc], [TR-03110-1]	The basic cryptographic function is provided by the Java Card OS platform (using a basic RSA operation). The protocol itself is implemented in the applet. (FCS_CKM.1.1/RSA-ENC)
6		Terminal Authentication v.1 for authentication of inspection system to travel documents's chip based on ECDSA using SHA-{1, 224, 256, 384, 512}	[TR-03111] (ECDSA), [FIPS180-4] (SHA)	160, 192, 224, 256, 320, 384, 512, 521 bit; elliptic curves brainpoolP{160, 192, 224, 256, 320, 384, 512}r1, brainpoolP{160, 192, 224, 256, 320, 384, 512}t1 [Brainpool], secp P-{160, 192, 224, 256, 384, 521}r1 [SEC2]	[TR-03110-1]	The basic cryptographic function is provided by the Java Card OS platform. The protocol itself is implemented in the applet. (FCS_COP.1.1/ECDS A-VERI, FCS_COP.1.1/HASH)

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Evaluator's Comments
7		Terminal Authentication v.1 for authentication of inspection system to travel documents's chip based on RSASSA-PSS using SHA-{1, 224, 256, 384, 512}	[RFC4056] (RSASSA-PSS), [FIPS180-4] (SHA)	Moduluslength = 512-2048 bit	[ICAODoc]	The basic cryptographic function is provided by the Java Card OS platform. The protocol itself is implemented in the applet. (FCS_COP.1.1/RSA-VERI, FCS_COP.1.1/HASH)
8		Active Authentication of the MRTD's chip based on RSA using SHA-{1,224,256,384,512 }	[ISO 9796-2] (RSA), [FIPS180-4] (SHA)	Moduluslength = 512-2048 bit	[ICAODoc]	The basic cryptographic function is provided by the Java Card OS platform. The protocol itself is implemented in the applet. (FCS_COP.1.1/RSA-SIGN, FCS_COP.1.1/HASH)
9		Active Authentication of the MRTD's chip based on ECDSA using SHA-{1,224,256,384,512 }	[TR-03111] (ECDSA), [FIPS180-4] (SHA)	160, 192, 224, 256, 320, 384, 512, 521 bit; elliptic curves brainpoolP{160, 192, 224, 256, 320, 384, 512}r1, brainpoolP{160, 192, 224, 256, 320, 384, 512}t1 [Brainpool], secp P-{160, 192, 224, 256, 384, 521}r1 [SEC2]	[ICAODoc]	The basic cryptographic function is provided by the Java Card OS platform. The protocol itself is implemented in the applet. (FCS_COP.1.1/ECDSA-SIGN, FCS_COP.1.1/HASH)

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Evaluator's Comments
10		Symmetric Authentication Mechanism based on AES for Personalization Agent	Standard equivalent to [ISO18013-3], AES following [FIPS197]	|k|=128, 192, 256	[ICAODoc] but with AES	The basic cryptographic function is provided by the Java Card OS platform. The protocol itself is implemented in the applet. (FCS_COP.1.1/AES)
11	Key Derivation	ECDH using SHA-{1, 256}	[ISO 15946] (ECDH), [FIPS180-4] (SHA), [ICAO_SAC]	160, 192, 224, 256, 320, 384, 512, 521 bit; elliptic curves brainpoolP{160, 192, 224, 256, 320, 384, 512}r1, brainpoolP{160, 192, 224, 256, 320, 384, 512}t1 [Brainpool], secp P-{160, 192, 224, 256, 384, 521}r1 [SEC2]	[TR-03110-1]	For PACE, Chip Authentication. [ICAO_SAC] implicitly contains the requirements for hash functions The basic cryptographic function is provided by the Java Card OS platform. The protocol itself is implemented in the applet. (FCS_CKM.1.1/ECC, FCS_COP.1.1/HASH)
12		DH using SHA-{1, 256}	[PKCS3] (DH), [FIPS180-4] (SHA), [ICAO_SAC]	Plength = 1024, 2048	[TR-03110-1]	For Chip Authentication The basic cryptographic function is provided by the Java Card OS platform (using a basic RSA operation). The protocol itself is implemented in the applet. (FCS_CKM.1.1/RSA-ENC)

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Evaluator's Comments
13	Confidentiality	AES in CBC mode	[FIPS197] (AES), [PKCS5] (CBC)	|k|=128, 192, 256	[ICAO_SAC]	FCS_COP.1/PACE_ENC FCS_COP.1.1/CA_ENC The cryptographic function is provided by the Java Card OS platform (FCS_COP.1.1/AES)
14		3DES in CBC mode	[FIPS46-3] (3DES), [PKCS5] (CBC)	|k|=112	[ICAO_SAC]	FCS_COP.1/PACE_ENC FCS_COP.1.1/CA_ENC The cryptographic function is provided by the Java Card OS platform (FCS_COP.1.1/3DES)
15	Integrity	AES in CMAC mode	[FIPS197] (AES), [NIST800-38B] (CMAC)	|k|=128, 192, 256	[ICAO_SAC] [TR-03110-1]	FCS_COP.1/PACE_MAC FCS_COP.1/CA_MAC The cryptographic function is provided by the Java Card OS platform (FCS_COP.1.1/CMA C-AES)
16		Retail-MAC	[FIPS46-3] (3DES), [ISO 9797-1] (Retail-MAC)	|k|=112	[ICAO_SAC] [TR-03110-1]	FCS_COP.1/PACE_MAC FCS_COP.1/CA_MAC The cryptographic function is provided by the Java Card OS platform (FCS_COP.1.1/MAC-DES)

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Evaluator's Comments
17	Trusted Channel	Secure messaging in ENC_MAC mode is established during PACE	[ICAO_SAC]	Cf. Confidentiality /Integrity	[ICAO_SAC] [TR-03110-1]	FIA_UAU.5/PACE The basic cryptographic function is provided by the Java Card OS platform. The protocol itself is implemented in the applet. (cf. Encryption and Integrity)
18		Secure messaging in ENC_MAC mode is established during Chip Authentication v1 after PACE	[ICAO_SAC]	Cf. Confidentiality /Integrity	[ICAO_SAC] [TR-03110-1]	FIA_UAU.5/PACE The basic cryptographic function is provided by the Java Card OS platform. The protocol itself is implemented in the applet. (cf. Encryption and Integrity)
19		Secure messaging for personalization	Standard equivalent to [ISO18013-3]	|k|=128, 192, 256	[ICAODoc] but with AES	The basic cryptographic function is provided by the Java Card OS platform. The protocol itself is implemented in the applet. (cf. Encryption
20	Crypto-graphic primitive	Deterministic RNG DRG.4	[AIS20]	–	–	FCS_RND.1 The cryptographic function is provided by the Java Card OS platform (FCS_RNG.1.1) The internal state of the RNG uses a PTRNG of class PTG.2 as a random source

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Evaluator's Comments
21	Key Generation	RSA Key Pair Generation for Active Authentication	[ISO 9796-2]	Moduluslength = 512-2048 bit	[ICAODoc]	FCS_CKM.1/AA The cryptographic function is provided by the Java Card OS platform.
22		ECC Key Pair Generation for Active Authentication	[ISO 15946]	160, 192, 224, 256, 320, 384, 512, 521 bit	[ICAODoc]	FCS_CKM.1/AA The cryptographic function is provided by the Java Card OS platform.

Table 4: TOE cryptographic functionality

For references used in Table 4 see standards as listed below:

[AIS20] AIS 20, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 15 März 2013

[Brainpool] RFC 5639 ECC Brainpool Standard Curves & Curve Generation, March 2010; available at: http://tools.ietf.org/html/rfc5639

[FIPS46-3] Federal Information Processing Standards Publication 46-3, DATA ENCRYPTION STANDARD (DES), Reaffirmed October 25, 1999, U.S. DEPARTMENT OF COMMERCE/National Institute of Standards and Technology

[FIPS180-4] Federal Information Processing Standards Publication 180-4 Secure Hash Standard (SHS), August 2015, Information Technology Laboratory National Institute of Standards and Technology

[FIPS197] Federal Information Processing Standards Publication 197, Announcing the ADVANCED ENCRYPTION STANDARD (AES), 2001-11-26, National Institute of Standards and Technology (NIST)

[ICAODoc] ICAO Doc 9303, Machine Readable Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006, International Civil Aviation Organization

[ICAO_SAC] International Civil Aviation Organisation, ICAO Machine Readable Travel Documents, Technical Report, Supplemental Access Control for Machine Readable Travel Documents, Version 1.01, 2010-11-11

[ISO15946] ISO 15946: Information technology – Security techniques – Cryptographic techniques based on elliptic curves, 2002

[ISO18013-3] ISO/IEC 18013-3:2009 Information technology – Personal identification - ISO-compliant driving licence - Part 3: Access control, authentication and integrity validation, 2009

[ISO 9796-2] ISO 9796-2: Information Technology – Security Techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms, 2002

[ISO 9797-1] Information technology - Security techniques - Message Authentication Codes (MACs) - Part 1: Mechanisms using a block cipher, 1999-12, ISO/IEC

[NIST800-38B] NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005, National Institute of Standards and Technology

[PKCS3] PKCS #3: Diffie-Hellman Key-Agreement Standard, Version 1.4, 1993-11-01, RSA Laboratories

[PKCS5] PKCS #5 v2.1: Password-Based Cryptography Standard, Version 2.1, 2006-10-05, RSA Laboratories

[RFC4056] Request for Comments: 4056, Use of the RSASSA-PSS Signature Algorithm in Cryptographic Message Syntax (CMS), J. Schaad, Soaring Hawk Consulting, June 2015

[SEC2] Standards for efficient cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters, Version 1.0, 2000-09-20, Certicom Research

[TR-03110-1] Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents, Part 1 - eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 2012-03-20, Bundesamt für Sicherheit in der Informationstechnik

[TR-03111] BSI - Technical Guideline, Elliptic Curve Cryptography, Version 2.0, 2012-06-28, Bundesamt für Sicherheit in der Informationstechnik

Note: End of report