Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1022-2018

for

NXP eDoc Suite v3.0 - cryptovision ePasslet Suite - Java Card applet configuration providing Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE

from

NXP Semiconductors Germany GmbH

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1022-2018 (*)

Electronic ID documents: IC with Applications

NXP eDoc Suite v3.0 - cryptovision ePasslet Suite - Java Card applet configuration providing Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE

from	NXP Semiconductors Germany GmbH
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 5 augmented by ALC_DVS.2 and AVA_VAN.5

SOGIS
Recognition Agreement

Common Criteria

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

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by 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.

Bonn, 18 May 2018
For the Federal Office for Information Security

Joachim Weber   L.S.
Head of Branch

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

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

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

- 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. 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 NXP eDoc 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 NXP eDoc 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 23 April 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: NXP Semiconductors Germany GmbH.

The product was developed by: cv cryptovision GmbH, Munscheidstr. 14, 45886 Gelsenkirchen, Germany.

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 May 2018 is valid until 17 May 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 NXP eDoc 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 Target of Evaluation (TOE) is a Java Card applet configuration providing a Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE option. The composite TOE is named *NXP eDoc 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 is intended for use as a Machine Readable Travel Document (MRTD) chip.

It consists of an applet configuration *ePasslet3.0/MRTD-EAC* provided by the *NXP eDoc 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. The TOE is available with different EEPROM sizes and in several variants which however are equivalent w.r.t. the evaluated security functionality.

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 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] and [9], 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
TSF_Access	Access Control
TSF_Admin	Administration
TSF_Secret	Secret key management
TSF_Crypto	Cryptographic operations
TSF_SecureMessaging	Secure Messaging
TSF_Auth	Authentication protocols
TSF_Integrity	Integrity protection
TSF_OS	Javacard OS Security Functionalities

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and [9], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], 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] and [9], 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:

NXP eDoc Suite v3.0 - cryptovision ePasslet Suite - Java Card applet configuration providing Machine Readable Travel Document with "ICAO Application", Extended Access Control with PACE

The following table outlines the TOE deliverables:

No.	Type	Item / Identifier	Version	Form of Delivery
1	HW+SW	*NXP eDoc Suite v3.0 – cryptovision ePasslet Suite* on platform *NXP JCOP 3 SECID P60 CS (OSB)*	3.0	Two different ways of delivery of the TOE are described. Either, the customer collects the product at the NXP site itself, or the product is sent by NXP to the customer. Here, the product is delivered in parcels sealed with special tapes to detect manipulation of the tapes.
2	DOC	*NXP eDoc 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)*	3.0.7	The TOE documentation is delivered in electronic form (encrypted) according to defined mailing procedures by NXP.

No.	Type	Item / Identifier	Version	Form of Delivery
3	DOC	*NXP eDoc 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)*	3.0.10	
4	DOC	*NXP eDoc Suite v3.0 – cryptovision ePasslet Suite – Java Card Applet Suite providing Electronic ID Documents applications Guidance Manual*	3.0.9	

Table 2: Deliverables of the TOE

The composite TOE consists of the underlying hardware platform, the crypto lib, the JCOP operating system and the *NXP 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. There the JCOP operating system and the applet is integrated into the ordered IC variant by masking during the chip production by the manufacturer, according to the configuration information contained in the OEF (Order Entry Form). 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 JCOP platform [14].

The TOE identification comprises several steps. The correctness of the IC and the existence of an additional banking applet can be checked with the custom mask ID by using GET DATA (Identify) command (see [20]).

The verification of the correct eDoc Suite version can be done by requesting data from the Issuer Security Domain by using GET DATA (Verify Package) command (see [20]).

Detailed information on the TOE identification can be found in the guidance documents for the TOE [11] [12] [13] and the platform [20].

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, and

- Protection of the TSF.

Specific details concerning the above mentioned security policies can be found in Chapter 6.2 of the Security Target [6] and [9].

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- OE.Auth_Key_Travel_Document,
- OE.Authoriz_Sens_Data,
- OE.Exam_Travel_Document,
- OE.Prot_Logical_Travel_Document,
- OE.Ext_Insp_Systems,
- OE.Legislative_Compliance,
- OE.Passive_Auth_Sign,
- OE.Personalisation,
- OE.Terminal,
- OE.Travel_Document_Holder,
- OE.Active_Auth_Key_MRTD,
- OE.APPLET,
- OE.VERIFICATION,
- OE.CODE-EVIDENCE,
- OE.APPS-PROVIDE,
- OE.VERIFICATION-AUTHORITY,
- OE.KEY-CHANGE,
- OE.SECURITY-DOMAINS,
- OE.USE_DIAG,
- OE.USE_KEYS, and
- OE.PROCESS_SEC_IC.

Details can be found in the Security Target [6] and [9], chapter 4.3 and in the guidance documents.

5. Architectural Information

The composite TOE, NXP eDoc 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 comprises of 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 JCOP 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 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

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

7. IT Product Testing

Developer's Test according to ATE_FUN

The developer's testing effort is summarised as follows:

TOE configurations tested:

The tests were performed with the composite smartcard product ePasslet3.0/MRTD-EAC on NXP JCOP 3 SECID P60 CS by NXP, in all variants as listed in [6, 1.1] (except the different memory configurations), i.e. with or without Mifare option and with or without an additional banking applet, including those used for the independent tests:

- J3H145CEX30,

- J3H145CAX30, and

- J3H145CGX30.

Developer's testing approach:

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

- Tests to cover all actions defined in [21],

- Good case and bad case tests for each command defined in the document [21] and executable on the TOE,

- Access rules test as part of the requirements on TSF data,

- Conformance tests according to BSI TR03105-Part3 with commercial test suites,

- Tests covering all TSF subsystems in the TOE design.

Verdict for the activity:

All test cases in each test suite were run successfully on this TOE version.

The developer's testing results demonstrate that the TOE performs as expected.

Independent Testing according to ATE_IND

The evaluator's testing effort is described as follows, outlining the testing approach, configuration, depth and results.

Test Approach and Set-up:

The TOE consists of the NXP eDoc 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 NXP JCOP 3 SECID P60 CS. The APDU tests were performed using standard PCSC 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 selected tests cover tests of the TSFI related to:

- Identification and Authentication (interfaces of different authentication mechanisms),

- Protection against interference, logical tampering and bypass (disturbance of interface execution),

- Secure Messaging (test of interface commands using secure messaging),

- Preparative procedures performed by the evaluator according to the guidance documentation [12] and [13].

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.

- Specific tests were conducted that were aligned during meetings with the certification body.

Configuration:

The TOE was tested in the HW variants:

- J3H145CAX30,

- J3H145CEX30, and

- J3H145CGX30.

All TOE variants were used for different tests with the ROM values, see [6, 1]. The keys and personalization data used in the test configurations were provided by the developer.

Test Results:

The test reports for the APDU tests are automatically generated by the test tool used. The test results are logged.

The test logs and the test documentation include details and comments on the test configuration, on the test equipment used, on the used command structure and the expected 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.

Penetration Testing according to AVA_VAN

Overview:

The penetration testing was performed at the site of the evaluation body TÜViT in the evaluator's test environment with the evaluator's test equipment. The samples were provided by the sponsor and by the developer. The test samples were configured and parameterized by the evaluator according to the guidance documentation. All configurations of the TOE being intended to be covered by the current evaluation were 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 of High was actually successful.

Penetration testing approach:

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment created within vulnerability analysis evaluation report, the evaluator created attack scenarios for penetration tests, where the evaluator is of the opinion, that the vulnerabilities could be exploitable. While doing this, the evaluator also considered all

aspects of the security architecture of the TOE, being not covered by the functional developer tests.

The source code reviews of the provided implementation representation accompanied the development of test cases and were used to find test input. The code inspection supported testing activity by enabling the evaluator to verify implementation aspects that could hardly be covered by test cases.

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

TOE test configurations:

The tests were performed with the one configuration of the TOE it is delivered in to the personalization agent, as stated in the security target.

Summary of Test Results and Effectiveness Analysis

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

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

There is only one configuration of the TOE. For all tests the TOE is configured and parameterized, if necessary, according to the guidance documents. The *ePasslet3.0/MRTD-EAC* TOE configuration is generated out of the applet suite that is part of the ROM of platform *NXP JCOP 3 SECID P60 CS (OSB)* by NXP. The *ePasslet3.0/MRTD-EAC* applet needs to be created according to the guidelines given in [12] 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:

- Application of CC to Integrated Circuits,
- Attack Methods for Smartcards and Similar Devices,
- Application of Attack Potential to Smartcards,
- Minimum Requirements for Evaluating Side-Channel Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations,

- Composite product evaluation for Smart Cards and similar devices (see AIS 36). According to this concept the relevant guidance documents of the underlying platform [20] and the documents ETR for Composition from the platform evaluations (i.e. [14] [15] [16] [17] [18] [19]) have been applied in the TOE evaluation.

(see [4], 26, 34, 36, 46).

For RNG assessment the scheme interpretations AIS 20 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 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: 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 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.

Since this TOE is a composite TOE it relies on its platform certifications. Please refer to [14][16][18] for details.

The composite TOE takes care of the recommendations and requirements imposed by the guidance documentation and ETR for composition of the underlying platform to be resistant against attackers with attack potential *high*.

In the course of the evaluation the underlying platform NXP JCOP 3 SECID P60 CS (OSB) underwent a re-certification and the re-certified platform was chosen as basis for the current composite evaluation. All composite work units according to [4, AIS36] were reworked and the evaluation reports are valid for the re-certified platform.

Further, the developer created an ST-Lite for publication. During the examination the evaluator compared the Security Target [6] with the Security Target Lite [9]. The Security Target Lite complies with the requirements of [4, AIS35]. Therefore the evaluator determines that the Security Target Lite is a correct sanitised version of the Security Target.

After completion of the evaluation report for aspect ALC the developer documents [9], [11], [12] were changed. The final version of the configuration list [10] which includes the current version of these documents was provided. The changes in the configuration list were examined and the evaluator is of the opinion that the evaluation report for aspect ALC remains valid also for the updated configuration list.

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

9.2. Results of cryptographic assessment

The table in annex C of part D of this report gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines the standard of application where its specific appropriateness is stated.

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

10. Obligations and Notes for the Usage of the TOE

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

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

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

11. Security Target

For the purpose of publishing, the Security Target [9] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12. Definitions

12.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
JCOP	Java Card Openplatform

MRED	Machine-Readable Etronic Document
MRTD	Machine-ReadableTravel Document
PACE	Password Authenticated Connection Establishment
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2. Glossary

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

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

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

13.   Bibliography

[1]   Common Criteria for Information Technology Security Evaluation, Version 3.1,
         Part 1: Introduction and general model, Revision 4, September 2012
         Part 2: Security functional components, Revision 4, September 2012

Part 3: Security assurance components, Revision 4, September 2012
http://www.commoncriteriaportal.org

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

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

[4]   Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[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-1022-2018, Version 1.7, 12 February 2018, NXP eDoc
Suite v3.0 - cryptovision ePasslet Suite – Java Card applet configuration providing
Machine Readable Travel Document with „ICAO Application" Extended Access
Control with PACE – Security Target, cv cryptovision GmbH (confidential document)

[7]   Evaluation Technical Report BSI-DSZ-CC-1023, Version 2, 16 March 2018, NXP
eDoc Suite v3.0 - cryptovision ePasslet Suite – Java Card applet configuration
providing Machine Readable Travel Document with „ICAO Application", Extended
Access Control with PACE, TÜV Informationstechnik GmbH – Evaluation Body for IT
Security (confidential document)

[8]   Protection Profiles PP-0056 and PP-0068: 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]   Security Target Lite BSI-DSZ-CC-1022-2018, Version 1.7, 22 February 2018, NXP
eDoc Suite v3.0 - cryptovision ePasslet Suite – Java Card applet configuration
providing Machine Readable Travel Document with „ICAO Application" Extended
Access Control with PACE – Security Target Lite, cv cryptovision GmbH (confidential
document) (sanitised public document)

[10]   Configuration list for the TOE, Revision 13027, 22 Februar 2018, File 2018-02-
22_conflist-JCOP3_rev13027.xlsx, cv cryptovision GmbH (confidential document)

[7]specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren

- AIS 26, Version 9, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document

- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

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

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

- AIS 36, Version 5, Kompositionsevaluierung including JIL Document and CC Supporting Document

- AIS 46, Version 3, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[11]   Guidance Document for the TOE: NXP eDoc 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, Version 3.0.7, 16 February 2018, cv cryptovision GmbH

[12]   Guidance Document for the TOE: NXP eDoc 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, Version   3.0.10, 20 February 2018, cv cryptovision GmbH

[13]   Guidance Document for the TOE: NXP eDoc Suite v3.0 – cryptovision ePasslet Suite – Java Card Applet Suite providing Electronic ID Documents applications Guidance Manual, Version 3.0.9, 26 February 2018, cv cryptovision GmbH

[14]   Certification Report NXP JCOP 3 SECID P60 CS (OSB), Report number NSCIB-CC-98209-CR2, version 2, 15 January 2018, TÜV Rheinland Nederland B.V.

[15]   Evaluation Technical Report for Composition NXP JCOP 3 SECID P60 CS (OSB) – EAL5+, version 3.0, 04 December 2017, Brightsight B.V. (confidential document)

[16]   Certification Report Crypto Library V3.1.x on P6022y VB, Certificate number CC-17-67206, Report number NSCIB-CC-67206-CR2, 17 November 2017, TÜV Rheinland Nederland B.V.

[17]   ETR for Composite Evaluation Crypto Library V3.1.x on P6022y VB EAL6+/5+, Reference 17-RPT-421, version 3.0, 24 October 2017, Brightsight B.V. (confidential document)

[18]   Certification report BSI-DSZ-CC-0973-V2-2016 for NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software, 11 October 2016, Bundesamt für Sicherheit in der Informationstechnik

[19]   Evaluation Technical Report for Composite Evaluation P6022y VB, version 1, 25 August 2016, TÜV Informationstechnik GmbH (confidential document)

[20]   Guidance Document for the platform: JCOP 3 SECID P60 CS User Guidance and Administration Manual, Rev. 2.5, 16 November 2017, NXP Semiconductors.

[21]   NXP eDoc 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 3.0.5, 29 September 2017, cv cryptovision GmbH (confidential document)

C.   Excerpts from the Criteria

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

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.4

- 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 C: Overview and rating of cryptographic functionalities implemented in the TOE

Annex B of Certification Report BSI-DSZ-CC-1022-2018

Evaluation results regarding development and production environment

The IT product NXP eDoc 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 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 May 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 <u>of the TOE</u> listed below:

a)   cv cryptovision GmbH, Munscheidstr. 14, 45886 Gelsenkirchen, Germany (software development site)

b)   Regarding the development and production sites of the platform, please refer to the certification reports NSCIB-CC-98209-CR2 [14], NSCIB-CC-67206-CR2 [16] and BSI-DSZ-CC-0973-V2-2016 [18].

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] and [9]) are fulfilled by the procedures of these sites.

Annex C of Certification Report BSI-DSZ-CC-1022-2018

Overview and rating of cryptographic functionalities implemented in the TOE

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
1	Authenticity	ECDSA-signature verification of card verifiable certificates using SHA-{1, 224, 256, 384, 512}	[ISO15946] (ECDSA), [FIPS180-4] (SHA)	160, 192, 224, 256, 320, 384, 512, 521 bit; elliptic curves brainpoolP{160, 192, 224, 256, 320, 384, 512}r1 [Brainpool], NIST P-{160, 192, 224, 256, 384, 521} [FIPS186-3]	[ICAODoc] (ECDSA), [TR-03110]	Verification of certificates for authenti-cation; FCS_COP.1/SIG_VER
2		RSASSA-PSS signature verification of card verifiable certificates using SHA-{1, 224, 256, 384, 512}	[PKCS1] (RSASSA-PSS), [FIPS180-4] (SHA)	Moduluslength = 2048 - 4096 bit	[ICAODoc] (RSA), [TR-03110]	Verification of certificates for authenti-cation; FCS_COP.1/SIG_VER
3	Authentication	PACE	[ICAO_SAC]	Length of MRZ or CAN, |Nonce|=128	[ICAO_SAC], [TR-03110]	FIA_UID.1/PACE, FIA_UAU.1/PACE
4		Chip Authentication v.1 for authentication of travel document's chip to inspection system based on ephemeral-static ECDH in combination with AES	[ISO15946] AES cf. Confidentiality/Integrity	Key sizes corresponding to the used elliptic curve brainpoolP{224, 256, 320, 384, 512}r1 [Brainpool], NIST P-{256, 384, 521} [FIPS186-3]	[ICAODoc], [TR-03110]	FIA_API.1
5		Chip Authentication v.1 for authentication of travel	[PKCS3], AES cf. Confidentiality/Integrity	Plength = 2048-4096	[ICAODoc], [TR-03110]	FIA_API.1

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
		document's chip to inspection system based on ephemeral-static DH in combination with AES				
6		Terminal Authentication v.1 for authentication of inspection system to travel document's chip based on ECDSA using SHA-{1, 224, 256,384, 512}	[ISO15946] (ECDSA), [FIPS180-4] (SHA)	Key lengths according to the elliptic curves brainpoolP{160, 192, 224, 256, 320, 384, 512}r1 [Brainpool], NIST P-{160, 192, 224, 256, 384, 521} [FIPS186-3]	[ICAODoc], [TR-03110]	FIA_UAU.5/PACE FCS_COP.1/SIG_VER
7		Terminal Authentication v.1 for authentication of inspection system to travel document's chip based on RSASSA-PSS using SHA-{1, 224, 256,384, 512}	[PKCS1] (RSASSA-PSS), [FIPS180-4] (SHA)	Moduluslength = 2048 - 4096 bit	[ICAODoc], [TR-03110]	FIA_UAU.5/PACE FCS_COP.1/SIG_VER
8		Active Authentication of the MRTD's chip based on RSA using SHA-{1, 224, 256, 384, 512}	[ISO9796-2] (RSA), [FIPS180-4] (SHA)	Moduluslength = 2048 - 4096 bit	[ICAODoc]	FCS_COP.1/SIG_GEN
9		Symmetric Authentication Mechanism based on AES for Personalization Agent	Standard equivalent to [ISO18013-3]	|k|=128, 192, 256	[ICAODoc] but with AES	-

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
10	Key Derivation	ECDH using SHA-{1, 256}	[ISO15946] (ECDH), [FIPS180-4] (SHA), [ICAO_SAC]	Key lengths according to the elliptic curves brainpoolP{160, 192, 224, 256, 320, 384, 512}r1 [Brainpool], NIST P-{160, 192, 256, 384, 521} [FIPS186-3]	[TR-03110]	For PACE and Chip Authent-ication. [ICAO_SAC] implicitly contains the requirements for hash functions; FCS_CKM.1/ DH_PACE, FCS_CKM.1/ CA
11		DH using SHA-{1, 256}	[PKCS3] (DH), [FIPS180-4] (SHA), [TR-03110], Annex A.1 (PACE).	Plength = 2048-4096	[TR-03110]	For Chip Authentication FCS_CKM.1/ CA
12	Confidenti ality	AES in CBC mode	[FIPS197] (AES), [NIST800-38A] (CBC)	|k|=128, 192, 256	[ICAO_SAC]	FCS_COP.1/P ACE_ENC FCS_COP.1.1 /CA_ENC
13		3DES in CBC mode	[FIPS46-3] (3DES), [NIST800-38A] (CBC)	|k|=112	[ICAO_SAC]	FCS_COP.1/P ACE_ENC FCS_COP.1.1 /CA_ENC
14	Integrity	AES in CMAC mode	[FIPS197] (AES), [NIST800-38B] (CMAC)	|k|=128, 192, 256	[ICAO_SAC], [TR-03110]	FCS_COP.1/P ACE_MAC FCS_COP.1/ CA_MAC
15		Retail-MAC	[FIPS46-3] (3DES), [ANSIX9.19] (RetailMAC)	|k|=112	[ICAO_SAC], [TR-03110]	FCS_COP.1/P ACE_MAC FCS_COP.1/ CA_MAC
16	Trusted Channel	Secure messaging in ENC_MAC mode establish during PACE	[ICAO_SAC]	Cf. Confidentiality/ Integrity	[ICAO_SAC], [TR-03110]	FIA_UAU.5/P ACE
17		Secure messaging in ENC_MAC mode is established during Chip Authenticatio n v1 after PACE	[ICAO_SAC]	Cf. Confidentiality/ Integrity	[ICAO_SAC], [TR-03110]	FIA_UAU.5/P ACE
18		Secure messaging for	Standard equivalent to [ISO 18013-	|k|=128, 192, 256	[ICAODoc] but with AES	For personalizatio n

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Standard of Application	Comments
		personalization	3]			
19	Cryptographic primitive	Deterministic RNG DRG.3	[AIS20]	n.a.	-	FCS_RND.1

Table 3: TOE cryptographic functionality

Note: End of report