Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0912-2014

for

cv act ePasslet Suite v2.1 – Java Card applet configuration providing Machine Readable Travel Document with “ICAO Application”, Extended Access Control (EAC)

from

NXP Semiconductors Germany GmbH

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0912-2014

Electronic ID documents: IC with Applications

cv act ePasslet Suite v2.1 – Java Card applet configuration providing Machine Readable Travel Document with "ICAO Application", Extended Access Control (EAC)

SOGIS
Recognition Agreement

from	NXP Semiconductors Germany GmbH
PP Conformance:	Machine Readable Travel Document with "ICAO Application" Extended Access Control, Version 1.10, 25 March 2009, BSI-CC-PP-0056-2009
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5

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 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.

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

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

Common Criteria
Recognition Arrangement
for components up to
EAL 4

Bonn, 22 December 2014

For the Federal Office for Information Security

Joachim Weber
Head of Division

L.S.

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

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

Contents

A. Certification

1. 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[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Technical information on the IT security certification, Procedural Description (BSI 7138) [3]
- BSI certification: Requirements regarding the Evaluation Facility (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1] also published as ISO/IEC 15408.
- 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]

2. 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.

2.1. European Recognition of ITSEC/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 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices

---

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

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

4 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

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

with Security Boxes" a SOGIS Technical Domains is in place, too. This Domain is linked to a conformance claim to one of the related SOGIS Recommended Protection Profiles. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

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

2.2. 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), certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

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 nations listed above.

As the product certified has been accepted into the certification process before 08 September 2014, this certificate is recognized according to the rules of CCRA-2000, i.e. up to and including CC part 3 EAL 4 components. The evaluation contained the components ALC_DVS.2 and AVA_VAN.5 that are not mutually recognised in accordance with the provisions of the CCRA-2000, for mutual recognition the EAL 4 components of these assurance families are relevant.

3. 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 cv act ePasslet Suite v2.1 – Java Card applet configuration providing Machine Readable Travel Document with “ICAO Application”, Extended Access Control (EAC) has undergone the certification procedure at BSI.

The evaluation of the product cv act ePasslet Suite v2.1 – Java Card applet configuration providing Machine Readable Travel Document with “ICAO Application”, Extended Access Control (EAC) was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 17 December 2014. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant is: NXP Semiconductors Germany GmbH.

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

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

4. Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only 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 levels please refer to the excerpts from the criteria at the end of the Certification 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-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 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.

5. Publication

The product cv act ePasslet Suite v2.1 – Java Card applet configuration providing Machine Readable Travel Document with “ICAO Application”, Extended Access Control (EAC), 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.

[6] Information Technology Security Evaluation Facility

Further copies of this Certification Report can be requested from the sponsor or the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] NXP Semiconductors Germany GmbH
Stresemannallee 101
22529 Hamburg
cv cryptovision GmbH
Munscheidstr. 14
45886 Gelsenkirchen

B. Certification Results

The following results represent a summary of

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

1. Executive Summary

The Target of Evaluation (TOE) is the composite TOE, named cv act ePasslet Suite v2.1 – Java Card applet configuration providing Machine Readable Travel Document with “ICAO Application”, Extended Access Control (EAC), and short named ePasslet2.1/MRTD-EACv1-BAC. It consists of an applet configuration ePasslet2.1/MRTD-EACv1-BAC provided by the cv act ePasslet Suite v2.1 used for electronic travel documents with EAC and BAC, the according guidance documents [10 and 11], the underlying operating system and the hardware platform with the crypto library. The operating system NXP JCOP 2.4.2 R3 (certificate ID: NSCIB-CC-13-37760-CR2) is provided in the following variants, that differ in connectivity (contactless/contact-based communication) and the memory size:

- J3E120_M65,
- J3E082_M65,
- J2E120_M65,
- J2E082_M65.

The hardware platform consists of the integrated circuit P5Cx145V0v (certificate ID: BSI-DSZ-CC-0858-2013) and the certified Crypto Library V2.7/2.9 (certificate ID: BSI-DSZ-CC-0750-V2-2014). 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 main security functionalities of the composite TOE are:

- EAC (Extended Access Control) and BAC functionality,[8]
- Administrative role authentication for storing manufacturing, pre-personalization and personalization data,
- Protection of integrity and confidentiality of internal applet and user data,
- Secure management and storage of secrets,
- Secure Messaging and implemented high level cryptographic functionality,
- Security functionalities provided by the underlying Crypto Library, IC and operating system.

The cv act ePasslet Suite v2.1 is a multi-application package for eID documents based on Java Card. It contains a fixed set of applications as stated in the Security Target [6], Table 1. These applications are realized by configurations of one or more predefined applets. While each application has a distinct configuration, different applications might use the same underlying applet.

[8] Please note that in consistency to the claimed protection profile the security mechanism Basic Access Control is not in the focus of this certification. The Basic Access Control mechanism was subject of the evaluation process BSI-DSZ-CC-0911-2014.

While the whole applet code resides in ROM, the applets providing the different applications are instantiated into EEPROM. Multiple applications can be present at the same time by instantiating multiple applets with their distinct configurations with some restrictions detailed below.

Combinations of certified and non-certified applications are possible. Via configuration the instantiated applets can be tied to the contactless and / or the contact interface, respectively. BAC, EACv1, EACv1-SAC require exclusive access to the contactless interface. Hence, if one of these applications is used (in certified configuration), further (certified or non-certified) applications have to be bound to the contact interface. The configuration of the TOE claimed by the Security Target [6] is fixed after personalization. Only applets of the cv act ePasslet Suite, which is part of the ROM mask, are available for the initial installation. Post issuance loading of applets is possible, but certain rules have to be followed as outlined in the user guidance documentation [10] and [11].

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, Version 1.10, 25 March 2009, BSI-CC-PP-0056-2009 [7].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. The SFRs are taken from the PP but complemented by product specific extensions . 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 rights
TSF_Admin	Administration
TSF_Secret	Secret key management
TSF_Crypto	Cryptographic operations
TSF_ SecureMessaging	Secure Messaging
TSF_Auth - TSF_Auth_Term - TSF_Auth_Sym - TSF_Auth_Chip - TSF_Auth_AA	Authentication protocols - Terminal Authentication - Symmetric authentication - Chip Authentication Protocol - Active Authentication Protocol
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], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3. 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.

The TOE is delivered before initialization / pre-personalization. The antenna is not part of the TOE, but the inlay holding the chip as well as the antenna and the booklet (holding the printed MRZ) are needed to represent a complete MRTD.

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:

cv act ePasslet Suite v2.1 – Java Card applet configuration providing Machine Readable Travel Document with "ICAO Application", Extended Access Control (EAC)

The following table outlines the TOE deliverables:

No	Type	Item	Identifier (Name and version) Description	Form of Delivery
1	HW/SW	Hardware-Chip with Applet Suite in ROM	cv act ePasslet Suite v2.1 on JCOP 2.4.2 R3 (J3E120_M65, J3E082_M65, J2E120_M65, J2E082_M65) , Mask ID 41h, Mask Name NX250Ah, Patch ID x1h, Target ID 01h This is the integrated circuit (in the form of module) with the embedded operating system and the cv act ePasslet Suite v2.1, ready for pre-personalization.	Secure physical delivery: Wafer, modules and packages (dice including identification T051A, T051B or sT051B)
2	DOC	cv act ePasslet/EACv1 Guidance Manual [10]	cv act ePasslet Suite v2.1 – Machine Readable Travel Document with „ICAO Application", Extended Access Control (EAC) – Guidance Manual v 3.1.7	Secure electronic delivery
3	DOC	JCOP Administrator Manual [11]	JCOP V2.4.2 Revision 3, JCOP V2.4.2 Revision 3 secure smart card controller, Administrator manual, Rev. 0.7, 2014-07-24, 258607, NXP The Guidance contains necessary information to pre-personalize the TOE.	Secure electronic delivery
4	KEYS	Keys	Transport key This key allows to access most parts of the EEPROM (including JCRE configuration area) to preconfigure the card. Authentication key This key allows to verify authenticity of the IC via internal JCOP authentication mechanism.	Secure electronic delivery

Table 2: Deliverables of the TOE

The composite TOE consists of the underlying hardware platform, the JCOP operating system and the ePasslet2.1/MRTD-EACv1-BAC applet. First the generated applet is delivered from the development to the production site, i.e. applet and guidance documentation delivery from cv cryptovision (developer) to NXP (manufacturer),

confidentiality and integrity is maintained by separate encrypted mails. 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 (before initialization / pre-personalization). The antenna is not part of the TOE. The pre-personalizer is responsible for the delivery of the pre-personalized hardware and the key material to the personalizer.

The delivery process is the same for the composite product as the delivery process is covered by the certified JCOP composite TOE. The Security Target [18] and the Administrator Guidance [11] of the JCOP platform outline the delivery procedure. Two different ways of TOE delivery are described. Either, the customer collects the product at the NXP site himself, or the product is sent by NXP to the customer. In that case the product is delivered in parcels sealed with special tapes to detect manipulation of the tapes. Also, a FAX is enclosed which the customer has to send back for verification of receiving an undamaged parcel.

The delivery of the documents and keys is performed by the document control office of NXP BU ID. The documents are delivered as encrypted PDF. The password required to open the document is delivered using a separate route of transport.

During the delivery of the applet and guidance documentation by cv cryptovision (developer) to NXP (manufacturer) confidentiality and integrity is maintained by separate encrypted mails.

In addition to the above mentioned methods of delivery and the according security mechanism, the correctness of delivery is ensured 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.

There are different mechanisms to verify the unique identity of the TOEs components according to the guidance documentation [10].

After selecting the applet with SELECT APDU, the version of the applet can be verified by the GET DATA APDU return value ‘iijj’ (Vii.jj=V1.13). The personalization options have to be read out by the GET DATA command and the parameters PO and OO can be checked against the expected values defined in the guidance documentation, which exactly describes the parameterization of the TOE, to verify the applet (ePasslet2.1/MRTD-EACv1-BAC configuration of the cv act ePasslet Suite v2.1).

With the IDENTIFY command, which is presented in the following table, it is possible to verify the identity of the TOE platform according to the JCOP guidance [11] (expected return values are marked with “ERV”):

The parameters for the IDENTIFY command are as follows:

Code	Value	Parameter setting
CLA	00h	ISO/IEC 7816-4
INS	A4h	SELECT command
P1	04h	Select by name
P2	00h	Select parameter
Lc	09h	Length of data field

Code	Value	Parameter setting
Le	00h	Expected length

Table 3: Parameters for the IDENTIFY command

The IDENTIFY command response and expected return values are as follows:

Offset	Size	Name	Base mask value	Comment
0	1	FABKEY ID	04h (Precise Biometrics) 05h (Neurotechnology)	“ERV” “ERV”
1	1	PATCH ID	x1h	“ERV”
2	1	TARGET ID	01h	“ERV”
3	1	MASK ID	40h (mask64) 41h (mask65) 42h (mask 66)	”ERV”
4	4	CUSTOM MASK	xxxxxxxxh	
8	6	MASK NAME	NX250Bh (mask64) NX250Ah (mask65) NX250Ch (mask66)	”ERV”
14	1	FUSED STATE	00h not fused 01h fused	“ERV”
15	1	ROM INFO LENGTH	03h	
16	3	ROM INFO[9]	784C6Ch (Precise Biometrics) D4B949h (Neurotechnology)	”ERV” ”ERV”
19	1	FIPS	01h if FIPS is enabled 00h if FIPS is disabled	“ERV”

Table 4: IDENTIFY command response and expected return values

In case that more than one application has been installed, each applet has to be selected and identified according to the respective guidance [10], [11].

3. Security Policy

The Security Policy of the TOE is defined according to the Protection Profile Machine Readable Travel Document with "ICAO Application" Extended Access Control, Version 1.10, 25 March 2009, BSI-CC-PP-0056-2009 [7] by the Security Objectives and Requirements for the contactless chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organisation (ICAO). The Security Policy addresses the advanced security methods in this Protection Profile according the 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

[9] ROM INFO: Checksum over the whole ROM of the chip. The checksum includes the JCOP OS and also any possibly available applets in a custom ROM mask.

specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- OE.MRTD_Manufact (Protection of the MRTD Manufacturing)
- OE.MRTD_ Delivery (Protection of the MRTD delivery)
- OE.Personalization (Personalization of logical MRTD)
- OE.Pass_Auth_Sign (Authentication of logical MRTD by Signature)
- OE.Auth_Key_MRTD (MRTD Authentication Key)
- OE.Authoriz_Sens_Data (Authorization for Use of Sensitive Biometric Reference Data)
- OE.BAC_PP (Fulfillment of the Basic Access Control Protection Profile)
- OE.Active_Auth_Key_MRTD (MRTD Active Authentication Key)
- OE.Exam_MRTD (Examination of the MRTD passport book)
- OE.Passive_Auth_Verif (Verification by Passive Authentication)
- OE.Prot_Logical_MRTD (Protection of data from the logical MRTD)
- OE.Ext_Insp_Systems (Authorization of Extended Inspection Systems)

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

5. Architectural Information

The TOE is an integrated circuit chip of machine readable travel documents (MRTD chip) programmed according to the Logical Data Structure (LDS) and providing the Basic Access Control and the Extended Access Control according to the ICAO document [19] and the technical guideline TR-03110 [20].

The TOE comprises eight subsystems, listed with a short description in the following:

- 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 instances 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 implement 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 subsystem 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 applet 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 challenges used.

The cv act ePasslet Suite v2.1 is a modular multi-application package for eID documents based on the Java Card standard. It provides the applications as stated in the Security Target [6], Table 1. These applications are realized by configurations of one or more predefined applets as described in the Security Target [6].

6. Documentation

The evaluated documentation [10] and [11] 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. Further documentation is provided to an applet developer as outlined in the certification report for JCOP [12].

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 developer's testing effort is summarized as follows:

TOE configurations tested: The tests were performed with the composite smartcard product ePasslet2.1/MRTDEACv1-BAC on JCOP 2.4.2R3 by NXP, in the variants J3E120/T0BE5076, J2E082/T0BE401, J3E120/T0BE4046, J2E082/T0BE505.

Developer's testing approach: The developer considered the following aspects when designing his test approach: Tests to cover all actions defined in Functional Specification (FSP); Good case and bad case tests for each command defined in the Functional Specification and executable on the TOE; Access Rules test as part of the requirements on TSF data; Conformance Tests according to BSI TR03105 [22] with commercial test suites; Tests covering all TSF subsystems in the TOE design.

All test cases in each test scenario were run successfully on this TOE version. The developers testing results demonstrate that the TOE performs as expected.

The evaluator's testing effort is summarized as follows:

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 ePasslet2.1/MRTD-EACv1-BAC application installed on NXP JCOP V2.4.2 R3. 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.

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 [10].

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 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 TSFI have been suitably tested. 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. All cryptographic functionality is provided by the platform and was sufficiently tested during platform evaluation. Specific tests were conducted that were aligned during meetings with the certification body.

Configuration: The TOE was tested in the variants J3E120/T0BE5076, J2E082/T0BE401, J3E120/T0BE4046, J2E082/T0BE505. 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 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:

The penetration testing was performed at the evaluators test environment with the evaluators test equipment. The samples were provided by the sponsor and partly configured by the developer. Additional test samples were configured and parameterized by the evaluator according to the guidance documentation. All configurations of the TOE 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 the evaluator created attack scenarios for penetration tests, where vulnerabilities could be exploitable. The evaluator also took the aspects of the security architecture of the TOE into account. The evaluator performed applet code analysis on his own during the composite activities, to verify that the developer has implemented all requirements of the underlying platforms for the composite TOE of the guidance documentation as well as of the security mechanisms of the applet in general. Further aspects, e.g. aiming the TSFI, are covered by the evaluator’s independent tests. The results of the evaluator activities led to confidence in the security of the TOE in a whole.

TOE test configurations: The tests were performed with the configuration of the TOE as it is delivered in to the personalization agent and stated in the security target. In those cases where no penetration tests have been performed, analysis due to non-exploitability of the related attack scenarios in the TOE's operational environment also including an attacker with an High attack potential have been performed. Certain LFI tests results on program flow of the other evaluations BSI-DSZ-CC-0913-2014 and BSI-DSZ-CC-0914-2014 were reused as they are also assignable to this TOE since they rely on the same platforms, code base and countermeasures.

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

8. Evaluated Configuration

The cv act ePasslet Suite v2.1 is a multi-application package for eID documents based on Java Card. It contains a fixed set of applications as stated in the Security Target [6], Table 1. These applications are realized by configurations of one or more predefined applets. While each application has a distinct configuration, different applications might use the same underlying applet.

While the whole applet code resides in ROM, the applets providing the different applications are instantiated into EEPROM. Multiple applications can be present at the same time by instantiating multiple applets with their distinct configurations with some restrictions detailed below.

Combinations of certified and non-certified applications are possible. Via configuration the instantiated applets can be tied to the contactless and / or the contact interface, respectively. BAC, EACv1, EACv1-SAC require exclusive access to the contactless interface. Hence, if one of these applications is used (in certified configuration), further (certified or non-certified) applications have to be bound to the contact interface. The configuration of the TOE claimed by the Security Target [6] is fixed after personalization. Only applets of the cv act ePasslet Suite, which is part of the ROM mask, are available for the initial installation. Post issuance loading of applets is possible, but certain rules have to be followed as outlined in the user guidance documentation [10], [11].

The TOE operating system platform is provided in certain variants that differ in connectivity (contactless / contact-based communication) and the memory size: J3E120_M65, J3E082_M65, J2E120_M65, J2E082_M65 as outlined in the platform certification [12].

Please note that in consistency to the claimed protection profile only the security mechanism Extended Access Control is in the focus of this certification.

Other certificates cover:

- the configuration providing Machine Readable Travel Document with „ICAO Application", Basic Access Control (BAC), BSI-DSZ-CC-0911-2014
- the configuration providing Machine Readable Travel Document with „ICAO Application", Extended Access Control with PACE, BSI-DSZ-CC-0913-2014
- the configuration providing Secure Signature Creation Device with key generation, BSI-DSZ-CC-0914-2014

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [8] 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 EAL5 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 (see [4], AIS 20, AIS 25, AIS 26, AIS 31, AIS 36):

- The Application of CC to Integrated Circuits,
- Application of Attack Potential to Smart Cards,
- Functionality classes and evaluation methodology for deterministic random number generators (for JCOP),
- Functionality classes and evaluation methodology for physical random number generators (for the hardware platform),
- Composite product evaluation for Smart Cards and similar devices. According to this concept the relevant documents ETR for Composition from the platform evaluations (i.e. on hardware, crypto library and JCOP) have been provided to the composite evaluator and used for the TOE evaluation.

A document ETR for composite evaluation according to AIS 36 has not been provided in the course of this certification procedure.

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

- All components of the EAL 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_DVS.2 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, Version 1.10, 25 March 2009, BSI-CC-PP-0056-2009 [7]
- for the Functionality: PP conformant plus product specific extensions Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant EAL 4 augmented by 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. Therefore, the evaluation and certification results of the underlying Java card platform NXP JCOP 2.4.2 R3 (certificate NSCIB-CC-13-37760-CR2 issued by the Netherlands CC Certification

Scheme NSCIB, [12]) including the Hardware platform certificate BSI-DSZ-CC-0858-2013 issued by BSI [14] and the Crypto Library certificate BSI-DSZ-CC-0750-V2-2014 issued by BSI [13] by applying the composite certification approach, too.

9.2. Results of cryptographic assessment

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

For details of the cryptographic algorithms that are implemented by the TOE to enforce its security policy please refer to chapter 8 of the Security Target [6]. The table outlines the Purpose, the Cryptographic Mechanism, the Standard of Implementation, the Key Size in bits and the Standard of Application. According to the Standard of Application noted, the algorithms are suitable for the intended usege. The validity period of the algorithms is mentioned in the german official catalogue [21].

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. Please bear in mind that the TOE is delivered before pre-personalization and the antenna is not part of the TOE. Also, the pre-personalization agent has to carefully follow the guidance [10] and all JCOP documentation that is part of the delivery of the TOE, i.e. [11], [12], [18].

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 9.2 has to be considered by the user and his system risk management process.

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

AIS Application Notes and Interpretations of the Scheme

ANSI American National Standards Institute

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
BU ID	A Business Unit of NXP
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
DTBS	Data To Be Signed
DTBS/R	DTBS Representation
EAC	Extended Access Control
EAL	Evaluation Assurance Level
EEPROM	Electronically Erasable Programmable Read Only Memory
ePKI	Electronic PKI
ETR	Evaluation Technical Report
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LDS	Logical Data Structure
MRTD	Machine Readable Travel Document
MRZ	Machine Readable Zone
OCR	Optical Character Recognition
OSP	Organisational Security Policy
PACE	Password Authenticated Connection Establishment
PDF	Portable Document Format
PKCS	Public-key cryptography standards
PKI	Public Key Infrastructure
PP	Protection Profile
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
SAC	Supplemental access control
SAR	Security Assurance Requirement
SCD	Signature Creation Data
SFP	Security Function Policy
SFR	Security Functional Requirement
SSCD	Secure Signature Creation Device

ST	Security Target
SVD	Signature Verification Data
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

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012

[3] BSI certification: Technical information on the IT security certification of products, protection profiles and sites (BSI 7138) and Requirements regarding the Evaluation Facility for the Evaluation of Products, Protection Profiles and Sites under the CC and ITSEC (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[10].

[5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0912-2014, cv act ePasslet Suite v2.1 – Java Card applet configuration providing Machine Readable Travel Document with „ICAO Application”, Extended Access Control (EAC) - Security Target Version 1.5, 1 October 2014, cv cryptovision

[7] Common Criteria protection profile: Machine Readable Travel Document with "ICAO Application" Extended Access Control, Version 1.10, 25 March 2009, BSI-CC-PP-0056-2009

[8] Evaluation Technical Report, Version 2, BSI-DSZ-CC-0912-2014, 27 November 2014, TÜV Informationstechnik GmbH (confidential document)

[9] Configuration list for the TOE BSI-DSZ-CC-0912-2014, 13 November 2014, cv cryptovision (confidential document)

[10] specifically

- AIS 1, Version 13, Durchführung der Ortsbesichtigung in der Entwicklungsumgebung des Herstellers
- 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 31, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL 5+ (CCv2.3 & CCv3.1) and EAL 6 (CCv3.1)
- AIS 36, Version 4, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.9, Reuse of evaluation results
- AIS 46, Version 2, Informationen zur Evaluierung von kryptographischen Algorithmen und ergänzende Hinweise für die Evaluierung von Zufallszahlengeneratoren

[10] cv act ePasslet Suite v2.1 – Machine Readable Travel Document with „ICAO Application", Extended Access Control (EAC) – Guidance Manual, V 3.1.7, 23 October 2014, cv cryptovision

[11] JCOP V2.4.2 Revision 3, JCOP V2.4.2 Revision 3 secure smart card controller, Administrator manual, Rev. 0.7, 24 July 2014, 258607, NXP

[12] Certification Report NXP J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65, and J2E082_M65 Secure Smart Card Controller Revision 3, version 1, 25 August 2014, TÜV Rheinland Nederland B.V., NSCIB-CC-13-37760-CR2

[13] Certification Report BSI-DSZ-CC-0750-V2-2014 for Crypto Library V2.7/2.9 on SmartMX P5Cx128/P5Cx145 V0v/ V0B(s) from NXP Semiconductors Germany GmbH, 16 July 2014

[14] Certification Report BSI-DSZ-CC-0858-2013 for NXP Secure PKI Smart Card Controllers P5CD128V0v/ V0B(s), P5CC128V0v/V0B(s), P5CD145V0v/ V0B(s), P5CC145V0v/ V0B(s), P5CN145V0v/V0B(s), each including IC Dedicated Software from NXP Semiconductors Germany GmbH, 12 June 2013, BSI

[15] ETR for Composite Evaluation NXP J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65, and J2E082_M65 Secure Smart Card Controller Revision 3 EAL5+, version 6, 12 August 2014, Brightsight (confidential document)

[16] ETR for composition Crypto Library V2.7/V2.9 on SmartMX P5Cx128/P5Cx145, according to AIS36, Brightsight 14-RPT-169, Revision 1.0, 26 June 2014 (confidential document)

[17] ETR for composition according to AIS36 on P5CD128V0A/B, P5CD128V0B(s), P5CC128V0A/B, P5CC128V0B(s), P5CD145V0A/B, P5CD145V0B(s), P5CC145V0A/B, P5CC145V0B(s), P5CN145V0A/B, P5CN145V0B(s), each including IC Dedicated Software, BSI-DSZ-CC-0858-2013, Version 1.0, 22 April 2013, T-Systems GEI GmbH (confidential document)

[18] NXP J3E145_M64, J3E120_M65, J3E082_M65, J2E145_M64, J2E120_M65, and J2E082_M65 Secure Smart Card Controller Revision 3, Security Target, Rev. 01.05, 2014-08-07, NSCIB-CC-13-37760-CR2, NXP

[19] International Civil Aviation Organization: ICAO Doc 9303, Machine Reada-ble Travel Documents, part 1 – Machine Readable Passports, Sixth Edition, 2006.

[20] Technical Guideline TR-03110:
BSI-TR-03110-1, Version 2.10, 20.03.2012, Advanced Security Mechanisms for Machine Readable Travel Documents – Part 1, BSI, https://www.bsi.bund.de/TR
BSI-TR-03110-2, Version 2.10, 20.03.2012, Advanced Security Mechanisms for Machine Readable Travel Documents – Part 2, BSI, https://www.bsi.bund.de/TR
BSI-TR-03110-3, Version 2.11, 12.07.2013, Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3, BSI, https://www.bsi.bund.de/TR

[21] BSI-TR-3116-2, eCard-Projekte der Bundesregierung, Teil 2, Hoheitliche Ausweisdokumente, BSI, https://www.bsi.bund.de/TR

[22] BSI TR-03105 Conformity Tests for Official Electronic ID Documents, BSI, https://www.bsi.bund.de/TR

C. Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model

Assurance Class	Assurance Components
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one

component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Evaluation assurance level 1 (EAL 1) - functionally tested (chapter 8.3)

“Objectives

EAL 1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL 1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL 1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL 1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL 2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering."

Evaluation assurance level 4 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs."

Evaluation assurance level 5 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques."

Evaluation assurance level 6 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL 6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs."

Evaluation assurance level 7 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

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

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0912-2014

Evaluation results regarding development and production environment

The IT product cv act ePasslet Suite v2.1 – Java Card applet configuration providing Machine Readable Travel Document with “ICAO Application”, Extended Access Control (EAC) (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 advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 22 December 2014, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1) are fulfilled for the development and production sites of the TOE listed below:

a) Developer, MRTD Manufacturer: cv cryptovision GmbH Munscheidstr. 14, 45886 Gelsenkirchen, Germany

b) For development and production sites regarding the platform please refer to the certification reports NSCIB-CC-13-37760-CR2 [12], BSI-DSZ-CC-0750-V2-2014 [13] and BSI-DSZ-CC-0858-2013 [14]

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.

This page is intentionally left blank.