Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0804-2012

for

cv act ePasslet/ePKI v3.6

from

cv cryptovision 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-0804-2012

Digital signature: Secure Signature Creation Devices (SSCD)

cv act ePasslet/ePKI v3.6

from	cv cryptovision GmbH
PP Conformance:	Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation, Dezember 2009, BSI-CC-PP-0059-2009
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by AVA_VAN.5

Common Criteria Recognition Arrangement for components up to EAL 4

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 guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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.

Bonn, 10 September 2012

For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED

Bernd Kowalski L.S.
Head of Department

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:

- BSIG[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 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- 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 technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In Addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

---

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

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.

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. 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.

This evaluation contains the component AVA_VAN.5 that is not mutually recognised in accordance with the provisions of the CCRA. For mutual recognition the EAL4 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/ePKI v3.6 has undergone the certification procedure at BSI.

The evaluation of the product cv act ePasslet/ePKI v3.6 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 23 August 2012. The 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.

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

[6] Information Technology Security Evaluation Facility

- 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.

5 Publication

The product cv act ePasslet/ePKI v3.6 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[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] cv cryptovision GmbH
Munscheidstr. 14
45886 Gelsenkirchen

This page is intentionally left blank.

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 contact-less integrated circuit chip containing the application cv act ePasslet/ePKI V3.6 for a secure signature creation device that can generate a signing key (signature creation data, SCD) and operates to create electronic signatures with the generated key.

The TOE is a combination of hardware and software configured to securely create, use and manage signature creation data. The TOE consists of

- the circuitry of the chip (the integrated circuit, IC) including the contact-based interface with hardware for the contact-less interface and the basic cryptographic software library, [9, 10, 11, 12, 13, 14, 18, 19, 20, 21, 22, 23],
- the platform with the Java Card operation system JCOP 2.4.1R3 by NXP, in the variants JxA081, A, B1, B4, Certification ID BSI-DSZ-CC-0675-2011; J2A080, Certification ID BSI-DSZ-CC-0674-2011; JxA040, A, B1, B4, Certification ID BSI-DSZ-CC-0730-2011, [15, 16, 17, 24, 25, 26],
- cv act ePasslet/ePKI v3.6,
- the associated Administrator and User Guidance [27] as well as JCOP documentation [28, 29, 30] (see details below).

The SSCD compliant configuration (application) cv act ePasslet/ePKI V3.6 is part of the cv act ePasslet Suite.

The TOE's functionality claimed by the Security Target [6] is realized by the cv act ePasslet/ePKI application as part of variant 1 (see Figure 1 of the Security Target [6]) on the chip platform P5Cx081 and of variant 2 (see Figure 2 of the Security Target [6]) on the chip platforms P5Cx080 and P5Cx040. PACE is only available in variant 1. The cv act ePasslet/ePKI application provides a PKCS15 compliant file structure and a separate DF for the SSCD functionality (D.Sig). While D.Sig provides the TOE's functionality, the PKCS15 part is out of scope of the certification. Some of the underlying platform variants of this composite TOE provide MIFARE functionality that are also out of scope of the TOE's security functionality. In the contact-less configuration the TOE additionally provides PACE for the establishment of a secure channel.

The SSCD protects the SCD during its whole life cycle as to be used in a signature-creation process solely by its signatory. The TOE provides the following functions:

- to generate signature creation data and the correspondent signature-verification data (SVD),
- to export the SVD for certification,
- to optionally receive and store certificate info,
- to switch the TOE from a non-operational state to an operational state, and
- if in an operational state, to create digital signatures for data with the following steps: a) select an SCD if multiple are present in the SSCD; b) receive data to be signed or a unique representation thereof (DTBS/R); c) authenticate the signatory and determine its intent to sign; d) apply an appropriate cryptographic signature-creation function using the selected SCD to the DTBS/R.

The TOE comprises all IT security functionality necessary to ensure the secrecy of the SCD and the security of the digital signature.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation, Dezember 2009, BSI-CC-PP-0059-2009 [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 AVA_VAN.5.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
TSF_Access	Access rights
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 functions

Table 1: TOE Security Functionality

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 cv act ePasslet Suite v1.1 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. For details on the relation between applets and applications please refer to Figure 1 and Figure 2 of the Security Target [6].

While the whole applet code resides in ROM, the applets providing the different applications are instantiated into EEPROM. A combination of several applications can be present at the same time by instantiating multiple applets with their distinct configurations with some restrictions detailed Figure 1 and Figure 2 of the Security Target [6]. A common combination could be e.g. an EACv1 applet and an ePKI applet providing a travel application with LDS data and EAC authentication together with a signature application.

The complete product (not to be mistaken for the TOE) is available in two variants.

Variant 1

- available on P5Cx081,
- covering all applications provided in Table 1 of the Security Target [6],
- certified products: BAC certified according to PP0055 (BSI-DSZ-CC-0798-2012, [33]), EACv1 certified according to PP0056 (BSI-DSZ-CC-0797-2012, [32]), EACv2-SAC certified according to SAC/PACE-PP (BSI-DSZ-CC-0799-2012, [34]), ePKI certified as Secure Signature Creation Device (SSCD) according to PP0059 (contact interface and contact-less interface with PACE) (BSI-DSZ-CC-0804-2012, [35]).

Variant 2

- available on P5Cx080 and P5Cx040,
- Contains the applets and applications indicated in Figure 2 of the Security Target [6],
- certified products: BAC certified according to PP0055 (BSI-DSZ-CC-0798-2012, [33]), EACv1 certified according to PP0056 (BSI-DSZ-CC-0797-2012, [32]), ePKI certified as Secure Signature Creation Device (SSCD) according to PP0059 (contact interface only) (BSI-DSZ-CC-0804-2012, [35]).

For this TOE (SSCD, ePKI) it means that TOE is available in the following two variants:

- Variant 1: Big ROM mask (includes PACE functionality) and
- Variant 2: Small ROM mask (does not include PACE functionality).

The small ROM mask does not include all available applets of the cv act ePasslet Suite v1.1. The PACE functionality is not available. Therefore only the contact interface can be used for variant 2 (small ROM mask).

This means for this TOE (SSCD, ePKI) that two variants are available on the following platforms:

Variant 1 (big ROM mask)

- JCOP 2.4.1R3 (JxA081, A, B1, B4) (Cert.-ID BSI-DSZ-CC-0675-2011, [17]) with crypto library v2.7 (Cert.-ID BSI-DSZ-CC-0633-2010, [14]) and hardware P5Cx081V1A (Cert.-ID BSI-DSZ-CC-0555-2009, [11]).

Variant 2 (small ROM mask)

- JCOP 2.4.1R3 (J2A080) (Cert.-ID BSI-DSZ-CC-0674-2011, [16]) with crypto library version 2.6 (Cert.-ID BSI-DSZ-CC-0709-2010, [13]) and hardware P5Cx080V0B (Cert.-ID BSI-DSZ-CC-0410-2010, [10]),
- JCOP 2.4.1R3 (JxA040, A, B1, B4) (Cert.-ID BSI-DSZ-CC-0730-2011, [15]) with crypto library version 2.7 (Cert.-ID BSI-DSZ-CC-0710-2010, [12]) and hardware P5Cx040VOB (Cert.-ID BSI-DSZ-CC-0404-2007, [9]).

Combinations of certified and non-certified applications are possible (as long as these applications use only the above applets instantiated from ROM). Via configuration the instantiated applets can be tied to the contact-less and/or the contact interface, respectively. BAC, EACv1, EACv2-SAC require exclusive access to the contact-less interface. Hence, if one of these applications is used (in a 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

installation. Additional applets cannot be loaded or installed. This explicitly excludes additional applet code being loaded and installed into EEPROM.

The TOE is delivered before pre-personalization/initialisation. The antenna is not part of the TOE.

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:

cv act ePasslet/ePKI v3.6

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 v1.1 on JCOP 2.4.1 R3 (JxA081, J2A080 or JxA040). This is the integrated circuit (in the form of module) with the embedded operating system and the cv act ePasslet Suite v1.1, ready for pre-personalization.	Secure physical delivery
2	DOC	cv act ePasslet/ ePKI Guidance [27]	cv act ePasslet/ePKI, cv act ePasslet Suite Java Card applet for PKI applications, Secure Signature Creation Device (SSCD) Configuration Guidance Manual, cv act ePasslet Suite version 1.1, cv act ePasslet/ePKI version 3.6, Document Version 1.0.1, 2012-06-11. The Guidance contains necessary information to pre-personalize and personalize the TOE.	Secure electronic delivery
3	DOC	JCOP Administrator Manual [28]	JCOP V2.4.1 Revision 3 Secure Smart Card Controller - Administrator manual, Rev. 3, 2011-03-08, NXP. The Guidance contains necessary information to pre-personalize the TOE.	Secure electronic delivery

No	Type	Item	Identifier (Name and version) Description	Form of Delivery
	DOC	JCOP User Manual [29]	JCOP V2.4.1 Revision 3 Secure Smart Card Controller - User Manual, Rev. 3.0, 9 March 2011, NXP. The Guidance contains necessary information to pre-personalize the TOE.	Secure electronic delivery
	DOC	NXP Application Note [30]	CV act ePasslet Suite V1.1, Pre-Personalization of JCOP JxA081EX0 products for cv act ePasslet Suite v1.1, Rev. 1.0, 28.11.2011, NXP. The NXP Application Note contains necessary information to pre-personalize the TOE.	Secure electronic delivery
	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

Delivery of the HW/SW items:

- The customer collects the hardware himself at the NXP site.
- The hardware is sent by NXP to the customer and protected by special measures.

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.

The TOE is delivered before pre-personalization/initialisation. 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.

NXP is responsible for the delivery of all needed documentation.

The identification of the TOE during the pre-personalization phase shall be performed by issuing the APDU command IDENTIFY. The returned ROM value has to match the platform, which includes all hardware and software (i.e. the used cv act ePasslet Suite v1.1). The identification procedure is described in detail in [27, chapter 2.2.3]. The following steps are a short summary:

- Boot the chip and send the IDENTIFY command: 00h A4h 04h 00h 09h A0h 00h 00h 01h 67h 41h 30h 00h FFh 00h
- Check if the returned ROM value matches the platform used as given below: Response (starting at byte offset 16): P5Cx081UA: 8F80EC; P5Cx080UA: 7C1970; P5Cx040UA: F39353

The identification of the TOE during the personalization phase shall be performed by issuing the APDU commands SELECT and GET DATA. This procedure is described in detail in [27, chapter 2.2.3]. The following steps are a short summary:

- Select ePKI applet using SELECT; Command: 00A40000 02 5015 00;
  Response: 6F228201388302501584 0CA000000063504B43532D313586080084848
  484FF84848A0105 9000
- Read out version information using GET DATA: Command: 00CA0182 02; Response:
  0306 9000
- Only for big ROM mask: Select ePAApplet using SELECT; Command: 00A40400 06
  D27600009801 00;
  Response:
  6F1C82013883023F008406D27600009801860800FF0CFFFFFF0C0C8A0103 9000
- Only for big ROM mask: Read out version information using GET DATA; Command:
  00CA0182 02; Response: 0108 9000

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

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It is defined according to the “Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation, Dezember 2009, BSI-CCPP-0059-2009” by the Security Objectives and Requirements for the Secure Signature Creation Device (SSCD) based on the requirements and recommendations 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 specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance:

- OE.SVD_Auth: Authenticity of the SVD
- OE.CGA_QCert: Generation of qualified certificates
- OE.SSCD_Prov_Service Authentic: SSCD provided by SSCD Provisioning Service
- OE.HID_VAD: Protection of the VAD
- OE.DTBS_Intend: SCA sends data intended to be signed
- OE.DTBS_Protect: SCA protects the data intended to be signed
- OE.Signatory: Security obligation of the Signatory

Details can be found in the Security Target [6], chapter 4.3

5 Architectural Information

The TOE is a combination of hardware and software configured to securely create, use and manage signature-creation data (SCD).

The TOE architecture of the cv act ePasslet Suite v1.1 comprises the following subsystems:

- Platform (S_Platform)
- Operating System (S_OpSys)
- Configuration Manager (S_CfgMgr)
- Event Manager (S_EvtMgr)
- Command Processor (S_CmdProc)
- Secure Messaging Manager (S_SecMsgMgr)
- File System Manager (S_FileSysMgr)
- State Manager (S_StateMgr)

The cv act ePasslet Suite v1.1 is a modular multi-application package for eID documents based on Java Card. 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 Figure 1 and Figure 2 of the Security Target [6].

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

The developer tested all TOE Security Functions on a simulator as well as on real cards. For all commands and functionality tests, test cases are specified in order to demonstrate its expected behaviour including error cases. Hereby a representative sample including all boundary values of the parameter set, e.g. all command APDUs with valid and invalid inputs were tested and all functions were tested with valid and invalid inputs. Partial repetition of developer tests was performed during the independent evaluator tests.

The independent tests of the evaluators were performed on the real cards. The self-protection of the TSF was tested by means of penetration tests. The tests of the evaluators covered aspects not already covered by the platform:

- Access Control (by means of APDU commands),
- Identification and Authentication (by means of APDU commands),
- Secure Messaging (by means of APDU commands),
- Preparative procedures, i.e. applet installing and personalisation (by means of APDU commands),
- Self-protection of TSF (by means of LFI),
- Resistance to Java Card related attacks (by means of source code review).

The evaluators have tested the TOE systematically against high attack potential during their penetration testing. The achieved test results correspond to the expected test results.

The selected tests cover tests of the TSFI related to

- Manufacturing (applet loading, installing and selection),
- 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,
- LFI tests using standard LFI equipment.

The choice of the subset of interfaces used for testing has been done according to the following approach:

- Augmentation of developer tests 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 TSFI 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 were 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 was based on evaluation experience of the evaluation body. Therefore all TOE security functionality was included within the subset. All cryptographic functionality is provided by the platform and was sufficiently tested during platform evaluation.

The TOE was tested on all hardware platforms. The keys and personalization data used in the test configurations were provided by the developer. The test reports for the APDU tests were 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.

The penetration testing was partially performed using the developer's testing environment, partially using the test environment of evaluator.

All configurations of the TOE that are covered by the evaluation were tested.

The evaluator devised penetration tests where the evaluator identified attack scenarios that could exploit potential vulnerabilities applicable to the TOE in its operational environment. This included

- Perturbation attacks on program flow disturbance and authentication bypass;
- Logical attacks on bypass authentication or access control;

- Reaching limits of resources or maximum values of parameters.

The evaluator performed code review of the cv act ePasslet Suite v1.1 to verify the implementation of the requirements of the platform's ETRs for composition and guidance as well as of the security mechanisms of the applets in general.

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

8 Evaluated Configuration

TOE is available in the following two variants:

- Variant 1: Big ROM mask (includes PACE functionality) and
- Variant 2: Small ROM mask (does not include PACE functionality).

The small ROM mask does not include all available applets of the cv act ePasslet Suite v1.1. The PACE functionality is not available. Therefore only the contact interface can be used for variant 2 (small ROM mask).

The two variants are available on the following platforms:

Variant 1 (big ROM mask)

- JCOP 2.4.1R3 (JxA081, A, B1, B4) (Cert.-ID BSI-DSZ-CC-0675-2011, [xx]) with crypto library v2.7 (Cert.-ID BSI-DSZ-CC-0633-2010, [xx]) and hardware P5Cx081V1A (Cert.-ID BSI-DSZ-CC-0555-2009, [xx]).

Variant 2 (small ROM mask)

- JCOP 2.4.1R3 (J2A080) (Cert.-ID BSI-DSZ-CC-0674-2011, [16]) with crypto library version 2.6 (Cert.-ID BSI-DSZ-CC-0709-2010, [13]) and hardware P5Cx080V0B (Cert.-ID BSI-DSZ-CC-0410-2010, [10]),
- JCOP 2.4.1R3 (JxA040, A, B1, B4) (Cert.-ID BSI-DSZ-CC-0730-2011, [15]) with crypto library version 2.7 (Cert.-ID BSI-DSZ-CC-0710-2010, [12]) and hardware P5Cx040VOB (Cert.-ID BSI-DSZ-CC-0404-2007, [9]).

Combinations of certified and non-certified applications are possible (as long as these applications use one of the above applets instantiated from ROM). Via configuration the instantiated applets can be tied to the contact-less and/or the contact interface, respectively. BAC, EACv1, EACv2-SAC require exclusive access to the contact-less 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 installation. Additional applets cannot be loaded or installed. This explicitly excludes additional applet code being loaded and installed into EEPROM.

The TOE is delivered before pre-personalization/initialisation. The antenna is not part of the TOE.

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:

- 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 libraries and JCOP) have been provided to the composite evaluator and used for the TOE evaluation.

(see [4], AIS 20, AIS 25, AIS 26, AIS 31, AIS 34, AIS 35, AIS 36, AIS 38 were used).

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

- All components of the EAL 4 package including class ASE as defined in the CC (see also part C of this report).
- The component AVA_VAN.5 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation, Dezember 2009, BSI-CC-PP-0059-2009 [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 AVA_VAN.5

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

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

9.2 Results of cryptographic assessment

The 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). This holds for the TOE Security Functionalites TSF_Crypto and TSF_OS and is detailed in the following table.

The table lists the cryptographic algorithms that are used by the TOE to enforce its security policy.

Algorithm	Bit Length	Purpose	Security Function	Standard of Implementation	Standard of Application
RSA	1976 - 2048	signature generation and verification	TSF_Crypto TSF_OS	PKCS1, v1.5	-
RSA CRT Key Generation	1976 - 2048	Key Generation	TSF_Crypto TSF_OS	PKCS1, v1.5	-
ECDSA	0	signature generation and verification	TSF_Crypto TSF_OS	ISO/IEC 14888-3	-
ECDSA Key Generation	224 – 320	Key Generation	TSF_Crypto TSF_OS	ANSI-X.9.62	-
SHA-224	-	signature generation	TSF_OS	FIPS PUB 180-4	-
SHA-256	-	signature generation	TSF_OS	FIPS PUB 180-4	-

Table 3: Cryptographic Algorithms used by the TOE

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 4, Para. 3, Clause 2). But Cryptographic Functionalities with a security level of 80 bits or lower can no longer be regarded as secure against attacks with high attack potential without considering the application context. Therefore for this functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

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.

Especially, after pre-personalization the selection of the card manager has to be disabled permanently by the pre-personalizer. This is described in the JCOP Administrator Manual [28], chapter 2.3.1.

Please bear in mind that the TOE is delivered before pre-personalization and the antenna is not part of the TOE. Therefore the pre-personalization agent has to carefully follow the guidance [27] and all JCOP documentation that is part of the delivery of the TOE, i.e. [28, 29, 30].

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 for the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms 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

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

ITSEC Information Technology Security Evaluation Criteria

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
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.

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

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

Informal - Expressed in natural language.

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

Protection Profile - An implementation-independent statement of security needs for a TOE type.

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 - A set of software, firmware and/or hardware possibly accompanied by guidance.

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 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8].

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

[6] Security Target cv act ePasslet/ePKI v3.6, BSI-DSZ-CC-0804, Version 1.05, Date 16.08.2012, cv cryptovision GmbH

[7] Protection Profile for Secure Signature Creation Device - Part 2: Device with Key Generation, Dezember 2009, BSI-CC-PP-0059-2009

[8] Evaluation Technical Report, cv act ePasslet/ePKI V3.6, Version 8, Date 22.08.2012, TÜV Informationstechnik GmbH (confidential document)

[9] Certification Report - BSI-DSZ-CC-0404-2007 for NXP Secure Smart Card Controller P5CD040V0B, P5CC040V0B, P5CD020V0B and P5CC021V0B each with specific IC Dedicated Software from NXP Semiconductors Germany GmbH Business Line Identification, 05.07.2007, BSI, including all Assurance Continuity Maintenance Reports

[10] Certification Report - BSI-DSZ-CC-0410-2007 for NXP Secure Smart Card Controller P5CD080V0B, P5CN080V0B and P5CC080V0B each with specific IC Dedicated Software from NXP Semiconductors Germany GmbH Business Line Identification, 05.07.2007, BSI, including all Assurance Continuity Maintenance Reports

[8] specifically

- AIS 20, Version 2, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 7, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 8,Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 2, 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 EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 35, Version 2.0, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 3, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.9, Reuse of evaluation results

[11] Certification Report - BSI-DSZ-CC-0555-2009 for NXP Smart Card Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A, P5CD041V1A, P5CD021V1A and P5CD016V1A each with IC dedicated Software from NXP Semiconductors Germany GmbH, 10.11.2009, including all Assurance Continuity Maintenance Reports

[12] Certification Report - BSI-DSZ-CC-0710-2010 for Crypto Library V2.6 on P5CD040V0B / P5CC040V0B / P5CD020V0B / P5CC021V0B / P5CD012V0B from NXP Semiconductors Germany GmbH, 07.01.2011, BSI

[13] Certification Report - BSI-DSZ-CC-0709-2010 for Crypto Library V2.6 on P5CD080V0B / P5CN080V0B / P5CC080V0B / P5CC073V0B from NXP Semiconductors Germany GmbH, 03.12.2010, BSI

[14] Certification Report - BSI-DSZ-CC-0633-2010 for Crypto Library V2.7 on P5CD081V1A / P5CC081V1A / P5CN081V1A / P5CD041V1A / P5CD021V1A / P5CD016V1A from NXP Semiconductors Germany GmbH, 19 November 2010, BSI, including reassessment dated 29.02.2012, BSI

[15] Certification Report - BSI-DSZ-CC-0730-2011 for NXP J3A040 & J2A040 Secure Smart Card Controller Revision 3 from NXP Semiconductors Germany GmbH, 25.05.2011, BSI

[16] Certification Report - BSI-DSZ-CC-0674-2011 for NXP J3A080 and J2A080 Secure Smart Card Controller Revision 3 from NXP Semiconductors Germany GmbH, 31.03.2011, BSI

[17] Certification Report - BSI-DSZ-CC-0675-2011 for NXP J3A081, J2A081 and J3A041 Secure Smart Card Controller Revision 3 from NXP Semiconductors Germany GmbH, 06.04.2011, BSI

[18] ETR for composition according to AIS36, NXP P5CD040V0B Secure Smart Card Controller, Version 1.4, 21.10.2011, T-Systems, Certification ID BSI-DSZ-CC-0404

[19] ETR for composition according to AIS36, NXP P5CD080V0B Secure Smart Card Controller, Version 1.31, 07.09.2010, T-Systems, Certification ID BSI-DSZ-CC-0410

[20] ETR for composition according to AIS36, NXP P5CD081V1A Secure Smart Card Controller, Version 1.4, 28.10.2011, T-Systems, Certification ID BSI-DSZ-CC-0555

[21] ETR for composition Crypto Library V2.6 on P5CD040V0B / P5CC040V0B / P5CD020V0B / P5CC021V0B / P5CD012V0B according to AIS36, 24.11.2010, Version 1.0, Certification ID BSI-DSZ-CC-0710, Brightsight

[22] ETR for composition Crypto Library Crypto Library V2.6 on P5CD080V0B / P5CN080V0B / P5CC080V0B / P5CC073V0B, 18.11.2010, Version 1.0, Certification ID BSI-DSZ-CC-0709, Project name Crypto Library V2.6 on P5CD080V0B / P5CN080V0B / P5CC080V0B / P5CC073V0B, Brightsight

[23] ETR for composition Crypto Library V2.7 on P5CD081V1A / P5CC081V1A / P5CN081V1A / P5CD041V1A / P5CD021V1A / P5CD016V1A, 27.02.2012, Version 5.0, Certification ID BSI-DSZ-CC-0633, Project name NXP CC CryptoLib P5CD081, Brightsight

[24] Evaluation technical report for composite evaluation, NXP J3A040 and J2A040 Secure Smart Card Controller Rev. 3, Version 3, 18.05.2011, TÜViT, Certification ID BSI-DSZ-CC-0730

[25] Evaluation technical report for composite evaluation, NXP J3A080 and J2A080 Secure Smart Card Controller Rev. 3, Version 2, 30.03.2011, TÜViT, Certification ID BSI-DSZ-CC-0674

[26] Evaluation technical report for composite evaluation, NXP J3A081, J2A081 and J3A041 Secure Smart Card Controller Rev. 3, Version 4, 06.04.2011-, TÜViT, Certification ID BSI-DSZ-CC-0675

[27] cv act ePasslet/ePKI, cv act ePasslet Suite Java Card applet for PKI applications, Secure Signature Creation Device (SSCD) Configuration Guidance Manual, cv act ePasslet Suite version 1.1, cv act ePasslet/ePKI version 3.6, Document Version 1.0.1, 11.06.2012, cv cryptovision GmbH

[28] JCOP V2.4.1 Revision 3 Secure Smart Card Controller - Administrator manual, Rev. 3, 08.03.2011, NXP

[29] JCOP V2.4.1 Revision 3 Secure Smart Card Controller - User Manual, Rev. 3.0, 09.03.2011, NXP

[30] CV act ePasslet Suite V1.1, Pre-Personalization of JCOP JxA081EX0 products for cv act ePasslet Suite v1.1, Rev. 1.0, 28.11.2011, NXP

[31] ICAO Doc 9303, Part 1, “Machine Readable Passports”, sixth edition, 2006, Part. 2, "Specifications for Electronically Enabled Passports with Biometric Identification Capability", and Part 3, “Machine Readable Official Travel Documents”, third edition, 2008, ICAO

[32] Certification Report - BSI-DSZ-CC-0797-2012 for cv act ePasslet/EACv1 v1.8 from NXP Semiconductors Germany GmbH, 2012, BSI

[33] Certification Report - BSI-DSZ-CC-0798-2012 for cv act ePasslet/BAC v1.8 from NXP Semiconductors Germany GmbH, 2012, BSI

[34] Certification Report - BSI-DSZ-CC-0799-2012 for cv act ePasslet/EACv2-SAC v1.8 from NXP Semiconductors Germany GmbH, 2012, BSI

[35] Certification Report - BSI-DSZ-CC-0804-2012 for cv act ePasslet/ePKI v3.6 from NXP Semiconductors Germany GmbH, 2012, BSI

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 9.4)

“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

Assurance Class	Assurance Components
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 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.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
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	2	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”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“Objectives

EAL1 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.

EAL1 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.

EAL1 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 EAL1 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 (EAL2) - structurally tested (chapter 8.4)

“Objectives

EAL2 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.

EAL2 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 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 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 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL4 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. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 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 (EAL5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL5 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 EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 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 (EAL6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL6 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.

EAL6 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 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL7 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 EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

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.”

This page is intentionally left blank

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 — see below

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0804-2012

Evaluation results regarding development and production environment

The IT product cv act ePasslet/ePKI v3.6 (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 10 September 2012, 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.1, 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

For development and production sites regarding the platforms please refer to the certification reports BSI-DSZ-CC-0404-2007 [9], BSI-DSZ-CC-0410-2007 [10], BSI-DSZ-CC-0555-2009 [11], BSI-DSZ-CC-0710-2010 [12], BSI-DSZ-CC-0709-2010 [13], BSI-DSZ-CC-0633-2010 [14], BSI-DSZ-CC-0730-2011 [15], BSI-DSZ-CC-0674-2011 [16], BSI-DSZ-CC-0675-2011 [17].

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.