Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0672-2010

for

Bundesdruckerei Document Application
Version 1.0.911

from

Bundesdruckerei 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-0672-2010

nPA Reader Device

Bundesdruckerei Document Application
Version 1.0.911

from	Bundesdruckerei GmbH
PP Conformance:	Common Criteria Protection Profile for Inspection Systems Version 1.01, 15 April 2010, BSI-CC-PP-0064-2010
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 3

Common Criteria Recognition Arrangement

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 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, 5 November 2010

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).

The new agreement was initially signed by the national bodies of Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom.

---

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

Within the terms of this agreement the German Federal Office for Information Security (BSI) recognises

- for the basic recognition level certificates issued as of April 2010 by the national certification bodies of France, The Netherlands, Spain and the United Kingdom.
- for the higher recognition level in the technical domain Smart card and similar Devices certificates issued as of April 2010 by the national certification bodies of France, The Netherlands and the United Kingdom.

In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

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

Historically, the first SOGIS-Mutual Recognition Agreement Version 1 (ITSEC only) became initially effective in March 1998. It was extended in 1999 to include certificates based on the Common Criteria (MRA Version 2). Recognition of certificates previously issued under these older versions of the SOGIS-Mutual Recognition Agreement is being continued.

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 January 2009 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 web site: 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.

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 Bundesdruckerei Document Application, Version 1.0.911 has undergone the certification procedure at BSI.

The evaluation of the product Bundesdruckerei Document Application, Version 1.0.911 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 29 October 2010. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Bundesdruckerei GmbH.

The product was developed by: Bundesdruckerei GmbH.

[6] Information Technology Security Evaluation Facility

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, where 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 Bundesdruckerei Document Application, Version 1.0.911 has been included in the BSI list of the 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] Bundesdruckerei GmbH
Oranienstraße 91
10958 Berlin
Deutschland

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 Bundesdruckerei Document Application, Version 1.0.911. It is a library, which is statically linked to an application running on an Inspection System (IS), called EAC-Box. The TOE is used to read and update the electronic data of the German identification card (“neuer Personalausweis (nPA)”) and verify the authenticity and the integrity of its data.

The TOE is applied in registration offices to allow citizens to verify that their nPA is working correctly. It is further possible to update the address information of the citizen, the citizen’s PIN for the eID application and the community ID (“Gemeindeschlüssel”). In addition, the eID application functionality of the nPA can be activated or deactivated.

Necessary protocols for the communication of the TOE with the electronic Machine Readable Travel Documents (eMRTD) like the nPA are described in [13] and [11].

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Common Criteria Protection Profile for Inspection Systems Version 1.01, 15 April 2010, BSI-CC-PP-0064-2010 [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 3.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. 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 Functionalities:

TOE Security Functionality	Addressed issue
SF.PROTOCOLS	Ensures the necessary protocols and cryptographic operations
SF.MANAGEMENT	Enforces the management functions for the administrator an the operator
SF.AUDIT	Generates audit data which is then stored by the environment

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 3.2. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.3 to 3.5.

This certification covers the following configurations of the TOE: TOE in version 1.0.911 and under consideration of version 1.4.17 of the rest of the firmware of the EAC-Box (including the Operating System).

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:

Bundesdruckerei Document Application, Version 1.0.911

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/SW	Software Library that works in the smart card terminal and that is delivered to the user together with the terminal or later via an update	1.0.911	Stored in the terminal or via update
2	DOC	Guidance documentation	1.4	download via secured web portal

Table 2: Deliverables of the TOE

Please note that additional smart cards are required for the administrator and operator of the terminal. However, the delivery of those cards is out of scope for this evaluation.

The terminal that operates the TOE is delivered to the user via standard delivery services (e.g. DHL). The delivery however, is tracked and the terminal can only be operated using an operator, administrator and revisor smart card which are shipped separately. For terminals that are already delivered to the customer, the update functionality may be used to deliver the TOE.

The guidance documentation is not delivered together with the terminal as this would allow an attacker to steal a packet and manipulate a terminal as well as the guidance. Instead, the guidance documentation is downloaded by the users via a secured web portal.

The guidance will inform the administrator about all important aspects that need to be checked for a secure delivery.

The guidance documentation informs the administrator about the security characteristics of an authentic terminal. The following aspects ensure the authenticity:

- A logo of Bundesdruckerei
- Two seals on the terminal
- The type information printed on the terminal
- The security characteristics of the box used for shipment
- The version of the software can be verified, this enables the authorized users Operator and Administrator to identify the TOE by its version number.

3 Security Policy

The TOE is used to read and update the electronic data of the German identification card (“Personalausweis (PA)”) and verify its authenticity and the integrity of its data.

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues: Use of the results of an identification and authentication mechanisms, acceptance of software updates, deletion of ephemeral data and the implementation of communication protocols.

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:

- Mechanisms to boot the EAC-Box
- Signed certificates
- Public Key Infrastructures
- Cryptographic mechanism
- Secure administration
- Trained user
- Secure operating environment
- Secure communication
- Shielded display
- Terminal integrity
- Correct date
- Protection of chip password
- Protection of key and certificate data

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

5 Architectural Information

The physical scope of the TOE can best be depicted by the following figure from the Security Target:

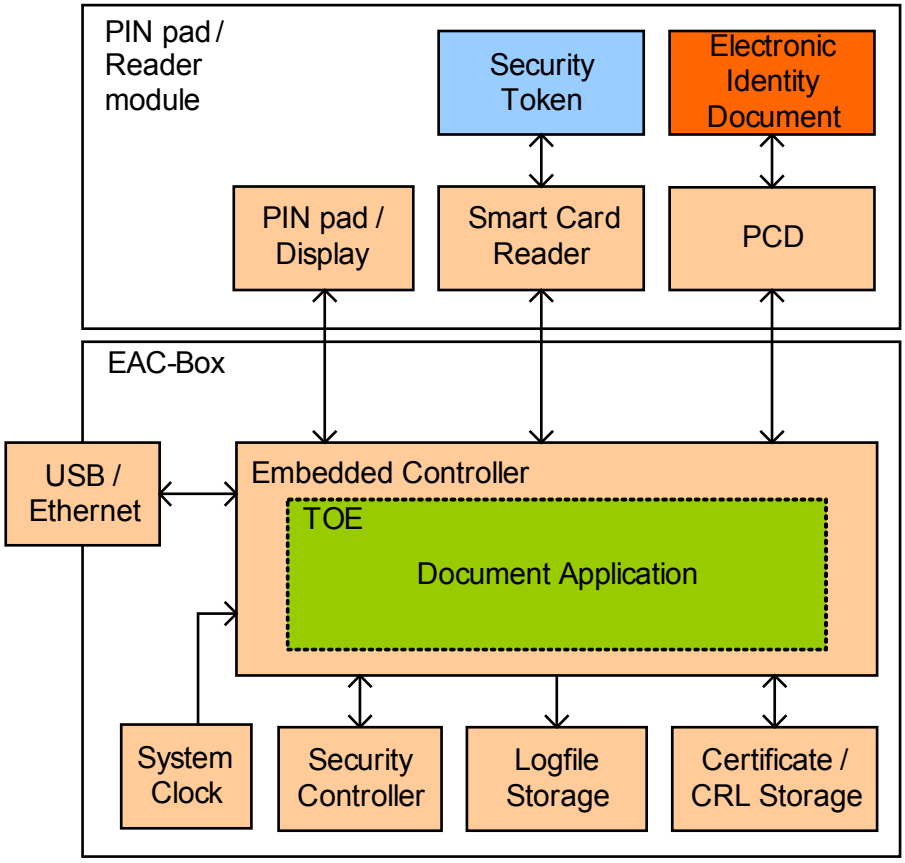

Figure 2: Scope and boundaries of the TOE

The TOE is the so called document application that is the core of the EAC Box, a smart card terminal to be used with the German Identity card. The TOE is software only that is executed within an Operating System/Firmware that belongs to the environment of the TOE.

The platform for the TOE is the Document Application Platform 1.0, which is based on a Linux Kernel of the 2.6 series and the GNU libc library. The underlying hardware is a 32 bit embedded controller.

The TOE relies on a security controller that performs the cryptographic operations for Terminal Authentication and that stores the necessary private key. All other cryptographic operations (e.g. for the other protocols) are performed in software by the TOE itself. Private keys that are used for other authentication mechanisms are stored temporarily in the volatile memory of the TOE.

Internally, the TOE can be structured according to the following subsystems from the TOE Design documentation.

Subsystem	Description
CRCTaskAssignment	Ensures that for each function call the correct role is active and handles the authentication context. After successful verification of the role the function calls are forwarded to CRC2.0

Subsystem	Descryption
CryptoLib	Cryptographic service provider
CRC2.0	Implements all relevant write and read permissions for the communication with the chip of an identity document.
CRCLogger	Creates and checks audit files. Logfiles are generated after a predefined scheme. The scheme for logging ensures the authenticity, order and completeness of audit data.
ReaderLib	Handles the communication with the reader and the chip of an identity document.
CRCSecurityController	Realizes certificate management and delivers certificates for Terminal Authentication and Passive Authentication. Realizes the signature functionality of Terminal Authentication.
CRCValidateUpdatePackage	Verifies the integrity and authenticity of software updates for the TOE.

Table 3: Overview of TOE structure

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

7.1 Exact Description of the Test configuration

As the TOE is a pure software application that is executed within an Operating System that runs on a smart card terminal the developer of the TOE chooses a software based concept for testing. They developed a dedicated test framework that links the TOE and that can then be run on the same hardware on which the TOE will be operated in practice.

This test configuration provides a dedicated test interface (based on SSH) that can be used to start test cases that are contained in the test framework. This is the only way to directly address the interfaces that the TOE provides during testing. The test cases of the developer cover the complete security functionality of the TOE.

The evaluator has chosen a four dimensional concept for testing:

1. All tests of the developer have been reviewed and executed again within the laboratory of TUViT

2. The evaluator modified test cases of the developer and developed additional test cases based on the test infrastructure of the developer in the course of independent testing.
3. As some of the security properties of the final TOE can only be judged for appropriateness using the final product, the evaluator tested the TOE using the final terminal and checked the behavior of the terminal against the guidance documentation.
4. The evaluator conducted penetration tests that made use of the test framework of the developer but also partly included direct manipulations of the environment of the TOE (even though such manipulations are not possible in practice due to dedicated assumptions in the Security Target).

7.1.1 Developer's Test according to ATE_FUN

TOE configuration tested:

- The tests were performed with the TOE in a special testing framework that was used to simulate the real operational environment.

Developer’s testing approach:

- Tests to cover the TSFI and their behavioural aspects defined in [FSP], by testing each command that can be sent to the TOE.
- Positive and negative tests are applied.
- Tests considering the different roles that can access the TOE.
- Tests covering all TSF subsystems in the TOE design.

Verdict for the activity:

- All test cases in each test scenario were run successfully on the TOE.
- The developer’s testing results demonstrate that the TOE performs as expected.
- All tests PASSED.

7.1.2 Evaluator Tests

7.1.2.1 Independent Testing according to ATE_IND

TOE configurations tested:

- C1: Standard test configuration - TOE within the test framework on the target Linux on ARM based hardware, as delivered to the final customer (identical to the test configuration of the developer)
- C2: Final configuration for delivery - TOE within the final delivered terminal with ARM hardware and terminal software and embedded Linux OS.

C1 is the standard configuration for all tests of the developer and the evaluator. C2 is the terminal in the final delivery state that is used for guidance testing and penetration testing of the evaluator.

Subset size chosen:

- The evaluators have tested each of the twelve commands of the two TSFI E.ADMIN and E.OPERATOR with C1. The configuration was used to cover usage of the TOE in the

final terminal. The evaluator chose to add tests for the usage of the TOE for the different user roles as defined in the guidance.

TSFI subset selection criteria:

- The evaluators have chosen to repeat all developer tests and to add tests for all TSFI with valid and invalid test cases. This approach covers the TOE functionality by invoking the complete set of interfaces and confirms that the TOE operates as specified.

TSFI tested:

- The evaluator tested the complete TSFI as documented in the functional specification.

Developer tests performed:

- The developer performed tests of all TSFI with an automated test framework running on the final hardware.
- The evaluator selected all tests of the developer's testing documentation for sampling due to the fact that all developer tests are implemented in scripts that can run without manual interactions.

Verdict for the activity:

- During the evaluator's testing the TOE operated as specified.
- The evaluators have verified the developer's test results by executing all of the developer's tests as documented in the test documentation.

7.1.2.2 Penetration Testing according to AVA_VAN

Overview:

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

There is only one configuration of the TOE under evaluation and addressed by testing.

The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential Basic has actually been successful.

Penetration testing approach:

Based on an initial list of potential vulnerabilities applicable to the TOE in its operational environment created within the work unit AVA_VAN.2-5 the evaluators devised the attack scenarios for penetration tests when they had the opinion that those potential vulnerabilities could be exploited in the TOE's operational environment.

While doing this, also the aspects of the security architecture described in ADV_ARC were considered for penetration testing. All other evaluation input was used for the creation of the tests as well. Specifically the test documentation provided by the developer was used to find out if there are areas of concern that should be covered by tests of the evaluation body.

As the TOE is a static library that heavily relies on the security measures of the environment (including the terminal in, which the TOE is integrated), the ARC document also covers some of the security measure that are applied by the terminal. The evaluator considered the fact that the TOE is delivered in such a way and widened the scope of the vulnerability analysis to cover specific security aspects of the whole terminal.

Furthermore, the evaluator came to an agreement with the developer to deliver those parts of the TOE source code that are developed by Bundesdruckerei. This code was analysed using a static code analysis tool. It should be noted that this procedure exceeds the required procedure for an EAL3 evaluation.

The evaluator also paid attention to the TSFI as outlined in the FSP. As the TSFI are quite simple with few options that can be varied and the TOE in deeply integrated into a terminal when it is delivered, the vulnerability assessment needed to focus on mechanisms that are operational inside the TOE or the terminal.

TOE test configurations:

- C1: *Standard test configuration* - TOE within the test framework on the target Linux on ARM based hardware, that is delivered to the final customer
- C2: *Final configuration for delivery* - TOE within the final delivered terminal with ARM hardware and terminal software and embedded Linux OS.

Verdict for the sub-activity:

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 Basic was actually successful in the TOE's operational environment as defined in [ST] provided that all measures required by the developer are applied.

Recommendation of the Evaluation Body:

The TOE is only a small part of the whole terminal and it heavily relies on the secure functioning of the rest of the terminal. **The overall security significantly depends on the secure environment in which the terminal is operated. Therefore, the evaluation body strongly advises that the responsible personnel is well trained to uphold security, i.e. secure operation, detection of manipulations, checking of seals, general security awareness.**

8 Evaluated Configuration

This certification covers the following configurations of the TOE:

Item	Exact version
TOE software	1.0.911
Rest of the terminal firmware (including the Operating System)	1.4.17

Table 4: Exact version information for the TOE

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [9] 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 RNG assessment the scheme interpretations AIS 20 was used (see [4]).

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

- All components of the EAL 3 package including the class ASE as defined in the CC (see also part C of this report)

The evaluation has confirmed:

- PP Conformance: Common Criteria Protection Profile for Inspection Systems Version 1.01, 15 April 2010, BSI-CC-PP-0064-2010
- for the Functionality: PP conformant plus product specific extensions Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant EAL 3

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 Functionality SF.PROTOCOLS and is detailed in the following table.

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

Algorithm	Bit Length	Purpose	Security Functionality	Standard of Implementation	Standard of Usage
Triple DES, CBC and CBC MAC	112	encryption / decryption / Key derivation	SF.PROTOCOLS	[11]	[11]
AES CBC and CMAC	128	encryption / decryption	SF.PROTOCOLS	[15], [16]	[11]
RSA	2048	Signature verification	SF.MANAGEMENT	[12]	[12]
ECDSA	256	Signature verification	SF.PROTOCOLS	[13]	[13]
SHA-1	160	Hash value computation	SF.PROTOCOLS	[14]	[11]
SHA-224	224	Hash value computation	SF.PROTOCOLS	[14]	[11]
SHA-256	256	Hash value computation	SF.PROTOCOLS	[14]	[11]
ECDH Signature verification		Key exchange	SF.PROTOCOLS	[11]	[11]

Algorithm	Bit Length	Purpose	Security Functionality	Standard of Implementation	Standard of Usage
PACE		Password authenticated key exchange	SF.PROTOCOLS	[11]	[11]

Table 5: TOE cryptographic functionality

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 4, Para. 3, Clause 2). According to Technical Guideline BSI-TR-03110, [11], the algorithms are suitable for securing originality and confidentiality of the stored data for machine readable travel documents (MRTDs). All cryptographic algorithms listed in table 5 are implemented by the TOE because of the standards building the TOE application (e.g. TR-03110 [11]). A validity period of each algorithm is not mentioned in BSI-TR-03110 [11]. For that reason an explicit validity period is not given.

10 Obligations and Notes for the Usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of assumptions, threats and policies 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.

If available, certified updates of the TOE shall be used. If non-certified updates or patches are available he should request the sponsor for providing a re-certification. In the meantime risk management process of the system using the TOE shall investigate and decide on the usage of not yet certified updates and patches or to take additional measures in order to maintain system security.

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

Beside or in order to highlight the information provided for TOE users (Administrator, Operator, and Revisor) in the guidance documentation the following hints and requirements have been of specific importance and are therefore mentioned here explicitly:

- The Security Target contains assumptions about the physical environment of the TOE. It is essential to understand that – even though the terminal that operates the TOE implements some very basic features for physical protection – the operators, administrators and revisors have to ensure that no unauthorized and unobserved access to the terminal that operates the TOE is possible.
- The terminals that operates the TOE shall be powered off every evening.
- The correct operation of the software environment of the TOE (i.e. the Operating System/Firmware) is of specific importance to the secure operation of the TOE. As such, the certificate for the TOE shall only be valid for the operation using the exact version of the Operating System/Firmware as it has been available during evaluation.

11 Security Target

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

12 Definitions

12.1 Acronyms

AES Advanced Encryption Standard

BSI Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany

BSIG BSI-Gesetz / Act on the Federal Office for Information Security

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Common Methodology for Information Technology Security Evaluation

DES Data Encryption Standard; symmetric block cipher algorithm

EAL Evaluation Assurance Level

eMRTD Machine Readable Travel Document

IT Information Technology

ITSEC Information Technology Security Evaluation Criteria

ITSEF Information Technology Security Evaluation Facility

MRTD Machine Readable Travel Document

nPA neuer Personalausweis

PP Protection Profile

SAR Security Assurance Requirement

SF Security Function

SFP Security Function Policy

SFR Security Functional Requirement

ST Security Target

TOE Target of Evaluation

Triple-DES Symmetric block cipher algorithm based on the DES

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, BSI 7149), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0672-2010, Version 2.7, 28.10.2010, Bundesdruckerei Document Application, Bundesdruckerei GmbH

[7] Common Criteria Protection Profile for Inspection Systems Version 1.01, 15 April 2010, BSI-CC-PP-0064-2010

[8] Evaluation Technical Report, Version 2, 29.10.2010, Bundesdruckerei Document Application 1.0.911, TÜV Informationstechnik GmbH, (confidential document)

[9] Configuration list for the TOE, Version 1.6, CI_Liste_Document_Application_v1.6.xls (confidential document)

[10] Guidance documentation for the TOE, Version 1.4, 27.10.2010, AGD - Document Application Guidance Documents, Bundesdruckerei GmbH

[11] Technical Guideline: Advanced Security Mechanisms for Machine Readable Travel Documents - Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.03, TR-03110, 2010

[12] Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, February 2003

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

[14] Federal Information Processing Standards Publication 180-3, Specifications for Secure Hash Standards (SHS), October 2008

[15] Federal Information Processing Standards Publication 197, Announcing the Advanced Encryption Standard (AES), November 26, 2001

[16] NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005

[8] specifically

- AIS 20, Version 1, 2. December 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 6, 3 August 2010, CC-Interpretationen im deutschen Zertifizierungsschema

C Excerpts from the Criteria

CC Part1:

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-

Assurance Class	Assurance Components
	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 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_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
ATE: Tests	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	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

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.

This page is intentionally left blank.