

# Certification Report

**BSI-DSZ-CC-0866-2013**

for

**IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0**

from

**Morpho B.V.**

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



# Deutsches IT-Sicherheitszertifikat

erteilt vom



Bundesamt für Sicherheit in der Informationstechnik

## BSI-DSZ-CC-0866-2013

### Ideal Pass v2 - SAC/EAC JC ePassport 4.0.0

from Morpho B.V.

PP Conformance: Common Criteria Protection Profile Machine Readable Travel Document with „ICAO Application“, Extended Access Control with PACE (EAC-PP) BSI-CC-PP-0056-V2-2012, Version 1.3.2, 5<sup>th</sup> December 2012

Functionality: PP conformant  
Common Criteria Part 2 extended

Assurance: Common Criteria Part 3 conformant  
EAL 5 augmented by  
ALC\_DVS.2 and AVA\_VAN.5



Common Criteria  
Recognition  
Arrangement  
for components up to  
EAL 4



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, 20 December 2013

For the Federal Office for Information Security

Joachim Weber  
Head of Division

L.S.



SOGIS Recognition  
Agreement

This page is intentionally left blank.

## Preliminary Remarks

Under the BSI<sup>1</sup> 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.

---

<sup>1</sup> Act on the Federal Office for Information Security (BSI-Gesetz - BSI<sup>1</sup>) of 14 August 2009, Bundesgesetzblatt I p. 2821

## Contents

A Certification.....	7
1 Specifications of the Certification Procedure.....	7
2 Recognition Agreements.....	7
3 Performance of Evaluation and Certification.....	8
4 Validity of the Certification Result.....	8
5 Publication.....	9
B Certification Results.....	11
1 Executive Summary.....	12
2 Identification of the TOE.....	13
3 Security Policy.....	14
4 Assumptions and Clarification of Scope.....	14
5 Architectural Information.....	14
6 Documentation.....	15
7 IT Product Testing.....	15
8 Evaluated Configuration.....	16
9 Results of the Evaluation.....	17
10 Obligations and Notes for the Usage of the TOE.....	19
11 Security Target.....	20
12 Definitions.....	20
13 Bibliography.....	22
C Excerpts from the Criteria.....	25
CC Part 1:.....	25
CC Part 3:.....	26
D Annexes.....	35

## A Certification

### 1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG<sup>2</sup>
- BSI Certification Ordinance<sup>3</sup>
- BSI Schedule of Costs<sup>4</sup>
- 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<sup>5</sup> [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.

---

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

<sup>3</sup> 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

<sup>4</sup> 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

<sup>5</sup> 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 components ALC\_DVS.2 and AVA\_VAN.5 that are 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 IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0, has undergone the certification procedure at BSI.

The evaluation of the product IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0, was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 2 December 2013. TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)<sup>6</sup> recognised by the certification body of BSI.

For this certification procedure the applicant is: Morpho B.V.

The product was developed by: Morpho B.V.

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

---

<sup>6</sup> 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.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

## 5 Publication

The product IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0, 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<sup>7</sup> of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

---

<sup>7</sup> Morpho B.V.  
P.O. Box 5300  
2000 GH Haarlem  
The Netherlands

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 "IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0", which is an electronic travel document (Machine Readable Travel Document – MRTD) representing a contactless/contact smart card integrated circuit, programmed according to ICAO Technical Report "Supplemental Access Control" [21] and the Logical Data Structure (LDS) defined in 'ICAO Doc 9303' [22]. The TOE provides additionally Extended Access Control according to the 'ICAO Doc 9303' [22] and BSI TR-03110 part 1 [25] and part 3 [26] and Active Authentication according to 'ICAO Doc 9303' [22]. The communication between terminal and chip shall be protected by Password Authenticated Connection Establishment (PACE) according to Electronic Passport using Standard Inspection Procedure with PACE (PACE PP), BSI-CC-PP-0068-V2 [10].

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Machine Readable Travel Document with „ICAO Application“, Extended Access Control with PACE (EAC PP), BSI-CC-PP-0056-V2-2012 [7]. The EAC PP is strict conformant to the Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011 [10]. In result, the TOE is also conformant to this PP.

Please note that in consistency to the claimed protection profile BSI-CC-PP-0056-V2-2012-MA-02 the security mechanisms Password Authenticated Connection Establishment and Extended Access Control are in the focus of this evaluation process. The ICAO Basic Access Control (BAC) security mechanism, which is also supported by the IDeal Pass v2 –SAC/EAC JC ePassport 4.0.0. product, is subject of the separate evaluation process BSI-DSZ-CC-0867.

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

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and Security Target Lite [8], 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 Functionality:

TOE Security Functionality	Addressed issue
SF I&A	Identification and Authentication
SF.CF	Cryptographic functions support
SF.ILTB	Protection against interference, logical tampering and bypass
SF.AC	Access control / Storage and protection of logical travel document data
SF.SM	Secure messaging
SF.LCM	Security and life cycle management

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] and Security Target Lite [8], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6] and Security Target Lite [8], chapter 3.1.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and Security Target Lite [8], chapter 3.2 to 3.4.

This certification covers the configurations of the TOE as outlined in chapter 8 (of this certification report).

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and 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:

### **IDEal Pass v2 - SAC/EAC JC ePassport 4.0.0**

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	The NXP J3E120_MP65 (JCOP 2.4.2R3) chip with the embedded software JCOP v2.4.2R3	ROM mask ID: 41h Patch level: 1 CI / Version of IDEal Pass v2 - SAC/EAC JC ePassport 4.0.0 applet loaded into EEPROM: 7103-9301-0311-1.0.59.300	Packed in sealed boxes, on sealed pallets with security transportation to the Personalization Agent
2	Keys	Personalization key set delivered separated from the TOE	7301-9310-605 7301-9311-605 7301-9312-605	Three key parts for each key, printed on separate forms and sent separately in sealed envelopes by registered mail to authorized key managers of the Personalization site
3	DOC	Preparative procedures [12]	1.1.0 / 7301-9301-504	Signed and encrypted (PGP) electronic document sent by email to the developer of the personalization system.
	DOC	Operational user guidance [13]	1.2.0/ 7301-9301-503	Secured email to the end customer (typically the MRTD issuing authority)

Table 2: Deliverables of the TOE

The TOE is finalised after initialisation / pre-personalisation and then delivered to the Personalisation site. If the Personalisation site is Morpho B.V. then pre-personalisation and

personalisation take place in the same security environment of the MRTD Manufacturing. If the TOE is delivered to a Personalisation site outside Morpho B.V. the delivery takes place as described in table 2 above.

### 3 Security Policy

The Security Policy of the TOE is defined according to the MRTD EAC/PACE PP [7] by the Security Objectives and Requirements for the contact-less and contact-based chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organisation (ICAO). The Security Policy addresses the advanced security methods for authentication and secure communication, which are described in detail in the Security Target [6] and Security Target Lite [8].

### 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.Legislative\_Compliance Issuing of the travel document
- OE.Auth\_Key\_Travel\_Document Travel document Authentication Key
- OE.Authoriz\_Sens\_Data Authorization for Use of Sensitive Biometric Reference Data
- OE.Passive\_Auth\_Sign Authentication of travel document by Signature
- OE.Personalisation Personalisation of travel document
- OE.Terminal Terminal operating
- OE.Travel\_Document\_Holder Travel document holder Obligations
- OE.Exam\_Travel\_Document Examination of the physical part of the travel document
- OE.Prot\_Logical\_Travel\_Document Protection of data from the logical travel document
- OE.Ext\_Insp\_Systems Authorization of Extended Inspection Systems

Details can be found in the Security Target [6] and Security Target Lite [8], chapter 4.2.

### 5 Architectural Information

The TOE consist of the following components:

- Smart Card Platform (Hardware Platform and Hardware Abstraction Layer);
- IC embedded software running on the Smart Card Platform consisting of the sub-systems:
  - Java Card virtual machine, ensuring language-level security;
  - Java Card runtime environment, providing additional security features for Java card technology enabled devices;
  - Java card API, providing access to card's resources for the Applet;

- Global Platform Card Manager, responsible for management of Applets on the card. For this TOE post issuance loading or deletion of Applets is not allowed;
- Native Mifare application, for this TOE the Mifare application is disabled;
- Ideal Pass v2 – SAC/EAC JC ePassport 4.0.0 applet which implements the eMRTD functionality.

## 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 Developer tests according to ATE\_FUN

The scenarios for performing the functional tests were structured top down by the TOE phases Manufacturing, Pre-Personalization, Personalization and Operational, added by some special test cases called command scans, destructive tests, media tests and perturbation and Morpho additional tests. The tests related to Pre-Personalization, Personalization and Operational life-cycle phases were subdivided into tests of the according APDUs, file handling, authentication mechanisms, and access conditions.

Most test cases started at applet instantiation or selection. Therefore the tested functionality includes successful execution of all necessary and preparative steps for the TOE configuration. The approach makes the tests repeatable and include aspects of regression tests.

The test prerequisites, test steps and expected results adequately test each TSFI. They are consistent with the descriptions of the TSFI in the functional specification.

The test plan includes all details about the set-up procedures, input parameters, the privileges to run, the test procedures and the test execution and is suitable to test the TSF mediated by the related interface adequately.

The internal interfaces are represented by and correspond to TSFI. All TSF subsystem and SFR-enforcing module behaviour is covered. The analysis of the test procedures show that all interfaces of SFR-enforcing modules are tested. All TSFI are covered and mapped to the tests. The testing approach allows to demonstrate that the interactions among subsystems work as described in the TOE design.

The actual test results correspond to the expected test results. The TOE has passed all tests so that all TSF listed above have been successfully tested against the assurance components ADV\_FSP.5 and ADV\_TDS.4. The developer's testing results demonstrate that the TSF perform as specified.

### 7.2 Independent evaluator tests according to ATE\_IND

The TOE and test configuration and the test tools are identical to the developer tests. Most tests performed with the test tool start at applet instantiation or selection which means that

most tests include successful execution of all previously necessary and preparative steps like personalization and configuration of the different authentication types.

Therefore the tests and their results were repeatable, the tests include aspects of regression, integration testing, negative tests, code inspection, stress tests, and electrical interface tests.

The 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.

The design of test cases and the choice of the subset of interfaces used for testing has been done including the repetition and augmentation of developer tests of interfaces and supplementation of the developer testing strategy for interfaces. The susceptibility to vulnerabilities of interfaces and related functionality was also a criterion.

The rigour of the tested interfaces is sufficient and the evaluator found that all TSFI are properly implemented.

The test prerequisites, test steps, and results are consistent with the descriptions of the TSFI in the functional specification. The actual test results correspond to the expected test results. The independent test results demonstrate that the TSF perform as specified.

### **7.3 Penetration Testing according to AVA\_VAN**

Based on the list of potential vulnerabilities applicable to the TOE in its operational environment attack scenarios for penetration tests were devised which could likely exploit the potential vulnerabilities in the TOE's operational environment. Within these activities also all aspects of the security architecture as described in ADV\_ARC which are not covered by functional testing, are considered.

The penetration tests were devised with the main focus on the potential vulnerabilities identified as applicable in the TOE's operational environment. An appropriate test set has been devised to cover these potential vulnerabilities.

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 actually successful in the TOE's operational environment as defined in [6] provided that all measures required by the developer are applied.

## **8 Evaluated Configuration**

This certification covers the following configurations of the TOE:

### **IDEal Pass v2 - SAC/EAC JC ePassport 4.0.0**

It comprises of:

- the NXP J3E120\_MP65 (JCOP 2.4.2R3) Secure Smartcard Controller, comprising of



- the circuitry of the MRTD's chip (the NXP P5CD145V0B integrated circuit, IC) with hardware for the contact and contactless interface;
- the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software;
- the IC Embedded Software (operating system): JCOP v2.4.2 R3;
- the MRTD application IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0 Applet version 1.0.59.300 loaded into EEPROM;
- the associated guidance documentation.

## 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 those components up to EAL5 extended by advice of the Certification Body for components beyond EAL5 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 (see [4], AIS 25),
- Application of Attack Potential to Smart Cards (see [4], AIS 26),
- Composite product evaluation for Smart Cards and similar devices (see AIS 36).  
*According to this concept the relevant guidance documents of the underlying platform and the documents ETR for Composition from the platform evaluations (i.e. on hardware [14], [15]) have been applied in the TOE evaluation.*

For RNG assessment the scheme interpretations AIS 20 was used (see [4]). The TOE uses platform for true random number generation, which provides random number generation in accordance with class DRG.3 of [4]

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

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

The evaluation has confirmed:

- PP Conformance: Protection Profile Machine Readable Travel Document with „ICAO Application“, Extended Access Control with PACE BSI-CC-PP-0056-V2-2012 [7]
- for the Functionality: PP conformant  
Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant  
EAL 5 augmented by ALC\_DVS.2 and AVA\_VAN.5

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

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 following table lists the cryptographic algorithms that are used by the TOE to enforce its security policy:

Algorithm	Bit Length	Application	Portion of the TSF	Implementation Standard	Application Standard	Comments <sup>8</sup>
TDES in CBC mode	[k]=112	en-/decryption	SF.CF.1	FIPS 46-3 (DES), SP 800-38A (CBC), ICAO 9303, Vol. 2, Appendix 5, A 5.3	ICAO 9303 [22], ICAO-SAC [21]	Used for PACE and CA TR-03110-3 [26]
TDES in Retail MAC mode	[k]=112	Key generation/ Key derivation	SF.CF.1	FIPS 46-3 (DES), ISO 9797 (Retail MAC)	ICAO 9303 [22], ICAO-SAC [21]	Used for PACE and CA TR-03110-3 [26]
AES in CBC mode	[k]=128, 192, 256	en-/decryption	SF.CF.1	FIPS 197 (AES) [31] SP 800-38A (CBC)	ICAO-SAC [21]	Used for PACE and CA TR-03110-3 [26]
AES in CMAC mode	[k]=128, 192, 256	Key generation/ Key derivation	SF.CF.1	FIPS 197 (AES) [31] SP 800-38A (CBC)	ICAO-SAC [21]	Used for PACE and CA TR-03110-3 [26]
TDES in CBC mode	[k]=112	Key generation/ Key derivation	SF.CF.6	-	ICAO 9303 [22], TR-03110-3 [26]	Used for PACE and CA TR-03110-3 [26]
SHA-1	-	PACE, CAv1, AA	SF.CF.2	FIPS180-2	ICAO-SAC [21], TR-03110-3 [26]	Used for key derivation, CAv1 [TR-3110], AA signature [ICAO]
SHA-224	-	AA	SF.CF.2	FIPS180-2	TR-03110-3 [26]	until 2015
SHA-256	-	PACE, CAv1, AA	SF.CF.2	FIPS180-2	TR-03110-3 [26]	until 2019
PACE	Length of MRZ or CAN, [Nonce]=128	Authenticated key derivation	SF.I&A.1	TR-3110-1 (PACEv2) [26]	ICAO-SAC [21], TR-03110-3 [26]	-
ECDH	Key sizes corresponding to the used elliptic curve brainpoolP{192, 224,256,320}r1 (RFC 5639), secp{192,224,25	Key derivation	SF.CF.5	ISO15946-3	ICAO-SAC [21], TR03110-3 [26]	Used for PACE and CA [TR-03110-3 [26]

<sup>8</sup> Information from TR-02102 [23] and Overview of Suitable Algorithms [24], if not referenced to other references

Algorithm	Bit Length	Application	Portion of the TSF	Implementation Standard	Application Standard	Comments
	6}r1 (SEC2) and ANSSI FRP256r1 Using SHA-{1, 256}					
Diffie-Hellman	plength= 2048 using SHA-{1, 256}	Key derivation	SF.CF.5	RSA-PKCS#3	ICAO-SAC [21], TR-03110-3 [26]	Used for PACE and CA TR-03110-3 [26]
RSA	RSA signature Modulus-length= 1536, 1792, 2048 using SHA-{1,224,256}	AA signature generation	SF.CF.3	ISO9796-2 (RSA)	ICAO 9303 [22]	Used for AA according to ICAO-9303
ECDSA	Key sizes 192, 224 256 and 320 bits supported used elliptic curves Brainpool 192r1, 224 r1, 256 r1, 320r1/ secp 192r1, 224r1,256r1 ANSI FRP256r1	AA signature generation	SF.CF.3	ISO15946-2 (ECDSA)	ICAO 9303 [22]	ECDSA: 224 bit until end of 2015, 256 bit until end of 2019
ECDSA	Key sizes 192, 224 256 and 320 bits supported used elliptic curves Brainpool 192r1, 224 r1, 256 r1, 320r1/ secp 192r1, 224r1,256r1 ANSI FRP256r1	Signature verification, TAv1	SF.CF.4	ISO15946-2 (ECDSA), FIPS 180-2 (SHA) ECDSA is according to [JCOP_ST] implemented in the platform according to ISO 14888-3 and FIPS 186-3.	(ECDSA), TR-03110-1 [25] (Brainpool-curves, NIST-curves), [ANSSI-Ref] (ANSSI FRP256r1)	ECDSA: 224 bit until end of 2015, 256 until end of 2019 SHA: 1, 224 bit until end of 2015, 256 until end of 2019 see [24]

Table 3: TOE cryptographic functionality

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). According to technical guideline BSI-TR-03110-1 [25] and ICAO 9303 [22] the algorithms are suitable to protect the authenticity (including integrity), authenticity, and confidentiality of the data stored on the radio frequency chip embedded in the travel document (MRTD chip).

The validity period of each algorithm is mentioned in the official catalogues [23 ] / [24].

## 10 Obligations and Notes for the Usage of the TOE

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

Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

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

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

## 11 Security Target

For the purpose of publishing, the Security Target [8] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

## 12 Definitions

### 12.1 Acronyms

<b>AIS</b>	Application Notes and Interpretations of the Scheme
<b>BAC</b>	Basic Access Control
<b>BSI</b>	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
<b>BSIG</b>	BSI-Gesetz / Act on the Federal Office for Information Security
<b>CCRA</b>	Common Criteria Recognition Arrangement
<b>CC</b>	Common Criteria for IT Security Evaluation
<b>CEM</b>	Common Methodology for Information Technology Security Evaluation
<b>EAC</b>	Extended Access Control
<b>EAL</b>	Evaluation Assurance Level
<b>ETR</b>	Evaluation Technical Report
<b>ICAO</b>	International Civil Aviation Organisation
<b>IT</b>	Information Technology
<b>ITSEF</b>	Information Technology Security Evaluation Facility
<b>MRTD</b>	Machine Readable Travel Document
<b>PACE</b>	Password Authenticated Connection Establishment
<b>PP</b>	Protection Profile
<b>SAR</b>	Security Assurance Requirement
<b>SFP</b>	Security Function Policy
<b>SFR</b>	Security Functional Requirement
<b>ST</b>	Security Target

<b>TOE</b>	Target of Evaluation
<b>TSF</b>	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** - A 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 4, September 2012  
Part 2: Security functional components, Revision 4, September 2012  
Part 3: Security assurance components, Revision 4, September 2012
- [2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012
- [3] BSI certification: Procedural Description (BSI 7125)
- [4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE<sup>9</sup>.
- [5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website
- [6] Security Target BSI-DSZ-CC-0866-2013, Version 1.2.5, Date: 2013-11-28, Security Target for the IDEal Pass v2 SAC/EAC JC ePassport 4.0.0, Morpho B.V. (confidential document)
- [7] Protection Profile Machine Readable Travel Document with „ICAO Application“, Extended Access Control with PACE BSI-CC-PP-0056-V2-2012, Version 1.3.2, 5th December 2012
- [8] Security Target BSI-DSZ-CC-0866-2013, Version 1.0.3, Date: 2013-11-28, Security Target Lite for the IDEal Pass v2 SAC/EAC JC ePassport 4.0.0, Morpho B.V. (sanitised public document)
- [9] Evaluation Technical Report, Version 3, Date: 2013-11-29, Project / Certification ID: 8109164033 / BSI-DSZ-CC-0866, TÜV Informationstechnik GmbH, (confidential document)
- [10] Protection Profile Machine Readable Travel Document using Standard Inspection Procedure with PACE, BSI-CC-PP-0068-V2-2011, Version 1.0, 2nd November 2011
- [11] Configuration list for the TOE, Version 1.1.2, Date: 2013-11-28, IDEal Pass v2 - SAC/EAC JC ePassport SAC/EAC configuration (confidential document)
- [12] Guidance documentation for the TOE, Version 1.1.0, Date: 2013-09-30, Preparative Guidance for the IDEal Pass v2 SAC/EAC JC ePassport v4.0.0, Morpho B.V.

---

<sup>9</sup>specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 8, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 9, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 35, Version 1, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 4, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2, Reuse of evaluation results

- [13] Guidance documentation for the TOE, Version 1.2.0, Date: 2013-09-27, Operational Guidance for the IDeal Pass v2 SAC/EAC JC ePassport v4.0.0, Morpho B.V.
- [14] Certification Report NXP J3E145\_M64, J3E120\_M65, J3E082\_M65, J2E145\_M64, J2E120\_M65, and J2E082\_M65 Secure Smart Card Controller Revision 3, NSCIB-CC-13-37760, August 12th, 2013, TÜV Rheinland Nederland B.V.
- [15] ETR for Composite Evaluation NXP J3E145\_M64, J3E120\_M65, J3E082\_M65, J2E145\_M64, J2E120\_M65, and J2E082\_M65 Secure Smart Card Controller Revision 3 EAL5+, report ID 13-RPT-208, NSCIB-13-37760, version 5.0, 9 August 2013, Brightsight
- [16] Certification Report Crypto Library V2.7/2.9 on SmartMX, P5Cx128/P5Cx145 V0v/ V0B(s) from NXP Semiconductors Germany GmbH, BSI-DSZ-CC-0750-2011, 11 April 2011, BSI
- [17] Assurance Continuity Maintenance Report, BSI-DSZ-CC-0750-2011-MA-02, Crypto Library V2.7/2.9 on SmartMX, P5Cx128/P5Cx145 V0v/ V0B(s) from NXP Semiconductors Germany GmbH, 04 July 2013, BSI
- [18] ETR for Composition Crypto Library V2.7 on NXP P5CD145V0A, MSO / P5CC145V0A, MSO / P5CD128V0A, MSO / P5CC128V0A, MSO according to AIS36, BSI-DSZ-CC-750, version 8.0, 02 August 2012, Brightsight
- [19] Certification Report BSI-DSZ-CC-0858-2013 for NXP Secure PKI Smart Card Controllers P5CD128V0v/ V0B(s), P5CC128V0v/ V0B(s), P5CD145V0v/ V0B(s), P5CC145V0v/ V0B(s), P5CN145V0v/V0B(s), each including IC Dedicated Software from NXP Semiconductors Germany GmbH, 12th June 2013, BSI
- [20] ETR for composition according to AIS36, P5CD128V0A/B, P5CD128V0B(s), P5CC128V0A/B, P5CC128V0B(s), P5CD145V0A/B, P5CD145V0B(s), P5CC145V0A/B, P5CC145V0B(s), P5CN145V0A/B, P5CN145V0B(s), each including IC Dedicated Software of NXP Semiconductors, BSI-DSZ-CC-858, Version 1.0, Date April 22th, 2013, T-Systems GEI GmbH
- [21] Machine Readable Travel Documents Technical Report, Supplemental Access Control for Machine Readable Travel Documents, International Civil Aviation Organization, Version 1.00, 11 November 2010
- [22] ICAO Doc 9303, Part 1, "Machine Readable Passports", Volume 2, "Specifications for Electronically Enabled Passports with Biometric Identification Capability" sixth edition, 2006, and Part 3, "Machine Readable Official Travel Documents", Volume 2, "Specifications for Electronically Enabled MRTDs with Biometric Identification Capability" third edition, 2008, ICAO
- [23] TR-02102, BSI – Technische Richtlinie, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2013.02, 09.01.2013, Bundesamt für Sicherheit in der Informationstechnik
- [24] Notification with regard to electronic signatures in accordance with the Electronic Signatures Act and the Electronic Signatures Ordinance( Overview of Suitable Algorithms) of 18 February 2013, To be published in Federal Gazette.
- [25] TR-03110-1, Technical Guideline TR-03110-1, Advanced Security Mechanisms for Machine Readable Travel Documents –Part 1 – eMRTDs with BAC/PACEv2 and EACv1, Version 2.10, 20.03.2012

- [26] TR-03110-3, Technical Guideline TR-03110-3, Advanced Security Mechanisms for Machine Readable Travel Documents – Part 3 – Common Specifications, Version 2.11, 12.07.2013
- [27] TR-03111, BSI – Technical Guideline, Elliptic Curve Cryptography, Version 2.0, 28.06.2012 Federal Office for Information Security
- [28] FIPS 180-4, Federal Information Processing Standards Publication FIPS PUB180-4, Secure Hash Standard (SHS), March 2012, Information Technology Laboratory National Institute of Standards and Technology
- [29] FIPS186-3, Federal Information Processing Standards Publication FIPS PUB 186-3, Digital Signature Standard (DSS), June 2009, U.S. department of Commerce / National Institute of Standards and Technology (NIST)
- [30] FIPS 197, Federal Information Processing Standards Publication 197, November 26, 2001, Announcing the ADVANCED ENCRYPTION STANDARD (AES), National Institute of Standards and Technology



## C Excerpts from the Criteria

CC Part 1:

### Conformance Claim (chapter 10.4)

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

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

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

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

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

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

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

CC Part 3:

**Class APE: Protection Profile evaluation** (chapter 10)

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

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

APE: Protection Profile evaluation class decomposition”

**Class ASE: Security Target evaluation** (chapter 11)

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

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

ASE: Security Target evaluation class decomposition

### Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.”

“Each assurance class contains at least one assurance family.”

“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation

Assurance Class	Assurance Components	
AGD:	AGD_OPE.1 Operational user guidance	
Guidance documents	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	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.
- Annex B: Evaluation results regarding development and production environment

This page is intentionally left blank.

## Annex B of Certification Report BSI-DSZ-CC-0866-2013

### Evaluation results regarding development and production environment



The IT product IDeal Pass v2 - SAC/EAC JC ePassport 4.0.0, (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 20 December 2013, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC\_CMC.4, ALC\_CMS.5, ALC\_DEL.1, ALC\_DVS.2, ALC\_LCD.1, ALC\_TAT.2)

are fulfilled for the development and production sites of the TOE listed below:

- a) Morpho B.V., Oudeweg 32, 2031 CC Haarlem, The Netherlands (Developer, MRTD Manufacturer)
- b) HID Global Ireland Teoranta Pairc Tionscail na Tulaigh, Baile na Abhann, Co.Galway, Ireland (Inlay Manufacturer)
- c) SMARTRAC TECHNOLOGY Ltd., Bangkok, Thailand, 142 Moo, Hi-Tech Industrial Estate, Tambon Ban Laean, Amphor Bang-Pa-In, 13160 Ayutthaya, Thailand (Inlay Manufacturer)
- d) PAV Card GmbH Hamburger Strasse 6, D-22952 Lütjensee, Germany (Inlay Manufacturer)

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [6]. The evaluators verified, that the threats, security objectives and requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and Security Target Lite [8]) are fulfilled by the procedures of these sites.

This page is intentionally left blank.