Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0643-2010

for

Sagem Identification EAC ePassport
Version 1.2.0

from

Sagem Identification bv

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-0643-2010

Security IC with MRTD EAC Application

Sagem Identification EAC ePassport
Version 1.2.0

from	Sagem Identification bv
PP Conformance:	Machine Readable Travel Document with "ICAO Application", Extended Access Control, BSI-PP-0026
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5

Common Criteria Recognition Arrangement for components up to EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 4 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, 04 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 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 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

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.

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 Sagem Identification EAC ePassport, Version 1.2.0 has undergone the certification procedure at BSI.

The evaluation of the product Sagem Identification EAC ePassport, Version 1.2.0 was conducted by TÜV Informationstechnik GmbH. The evaluation was completed on 03. November 2010. The TÜV Informationstechnik GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

[6] Information Technology Security Evaluation Facility

For this certification procedure the sponsor and applicant is: Sagem Identification bv.

The product was developed by: Sagem Identification bv.

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.

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 Sagem Identification EAC ePassport, Version 1.2.0 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] Sagem Identification bv
P.O. Box 5300
2000 GH Haarlem
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 contact-less integrated circuit of machine readable travel documents (MRTD's chip) supplied with a file system according to the Logical Data Structure (LDS) and providing the Basic Access Control according to the ICAO document [16], Active Authentication according to the ICAO document [16], and the Extended Access Control (Chip Authentication and Terminal Authentication) according to the technical report [17].

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, BSI-PP-0026 [7].

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

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [8], chapter 6. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Function	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 MRTD data
SF.SM	Secure Messaging
SF.LCM	Security and life cycle management

Table 1: TOE Security Functions

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

The assets to be protected by the TOE are defined in the Security Target [6] and [8], chapter 3.1.1. 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] and [8], chapters 3.2 to 3.4.

This certification covers the following configuration of the TOE (For details refer to chapter 8 of this report):

- The NXP J3A080 Secure Smartcard Controller Revision 2 (also named JCOP v2.4.1), comprising of (a) the circuitry of the MRTD's chip (the NXP P5CD080V0B integrated circuit) with hardware for the contact-less interface; (b) the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software; (c) the IC Embedded Software (operating system) JCOP v2.4.1 Revision 2;
- the MRTD application: Sagem Identification EAC ePassport version 1.2.0;

● the associated guidance documentation.

Only one application will be present on the IC, namely the MRTD Application. The TOE utilises the evaluation of the underlying platform, which includes the NXP chip, the IC Dedicated Software, and the JCOP v2.4.1 (Certification BSI-DSZ-CC-0597-2010 [15]).

The hardware platform NXP P5CD080V0B is certified by BSI (BSI-DSZ-CC-0410-2007, [13]) and the crypto libraries in the hardware are certified by BSI (BSI-DSZ-CC-0417-2008, [14]).

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:

Sagem Identification EAC ePassport version 1.2.0

The following table outlines the TOE deliverables:

No	Type	Description, Name	Version/Product ID (see also [11], chapter 2.1)	Form of Delivery
1	HW / SW	The NXP J3A080 Revision 2 chip with the embedded software JCOP v2.4.1 and the MRTD EAC application		Packed in sealed boxes, on sealed pallets with security transportation to the Personalization Agent
		ROM mask Code	49	
		Patch level	6	
		Product Identification / Applet CI-number and version	1.2.0 / 8158-8100-0308 00.06.07.0198	
2	KEY	The personalization key set, consisting of three key parts, delivered separated from the TOE	8158-8118-605 8158-8119-605 8158-8120-605	Sent separately by registered mail to the Personalization Agent
3	DOC	Preparative procedures [11]	2.0.6 / 8158-8103-504	Signed and encrypted (PGP) of the electronic document by email to the developer of the personalization system.
4	DOC	Operational user guidance [12]	2.0.2 / 8158-8101-503	Sent to the end customer (typically the MRTD issuing authority) by secured email

Table 2: Deliverables of the TOE

The TOE is finalized at the end of phase 2 according to the Protection Profile [7].

The delivery of the initialized and pre-personalized inlays is done in a secure way using sealed boxes and pallets via a security transport from the MRTD Manufacturer (Sagem Identification bv) to the Personalization Agent.

The TOE is protected by a personalization key. The Personalization Agent can only access the MRTD using the securely delivered keys. The personalization keys are generated at Sagem Identification bv in accordance with the key generation procedure. Each key is split-up in three parts, which are printed on separate forms. The key forms are sent separately by registered mail to the Personalization Agent. The Personalization Agent loads the keys into the HSM of the personalization system, in accordance with the Preparative Procedures [11]. For the delivery of the personalization key set and the guidance documents confidentiality and integrity have to be ensured. The Preparative Procedures [11] describe all procedures which have to be performed during personalization by the Personalization Agent. The Personalization Agent can verify the TOE identification using the GET INFO command.

3 Security Policy

The Security Policy of the TOE is defined according to the MRTD EAC PP [7] by the Security Objectives and Requirements for the contact-less chip of machine readable travel documents (MRTD) based on the requirements and recommendations of the International Civil Aviation Organisation (ICAO). The Security Policy address the advanced security methods Basic and Extended Access Control as well as Chip Authentication, and Active Authentication.

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:

- Assurance Security Measures in Development and Manufacturing Environment,
- Control over MRTD Material,
- Personalization of logical MRTD,
- Authentication of logical MRTD by Signature,
- MRTD Authentication Key,
- Authorization for Use of Sensitive Biometric Reference Data,
- Examination of the MRTD passport book,
- Verification by Passive Authentication,
- Protection of data of the logical MRTD,
- Authorisation of Extended Inspection Systems.

Details can be found in the Security Target [6] and [8], chapter 4.2 and 4.3.

5 Architectural Information

The TOE is a composite product. It consists of a secure Integrated Circuit (IC) with hardware for the contact-less interface, the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software, the IC Embedded Software (operating system) JCOP v2.4.1 Revision 2, and the MRTD application which is the Sagem Identification EAC ePassport Applet.

The applet is implemented in Java Card compatible Java. It consists of several classes / subsystems but most functionality of the TOE is part of a single class / subsystem, i.e. the EacApplet class. This EacApplet class is divided into several modules. The modules cover the implementation and handling of the authentication mechanisms, e.g. Chip Authentication, Active Authentication or Terminal Authentication, the handling of APDU commands of the phases before operational use phase, e.g. of Pre-Personalization and Personalization, phase spanning mechanisms as Secure Messaging as well as overall attack preventing modules, e.g. a perturbation module.

The EACApplet uses the provided functionality of the JCOP platform as defined by the JavaCard specification and the JCOP design, i.e. the specified APIs and libraries. Insofar the JCOP platform acts as a software layer.

6 Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

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

7 IT Product Testing

The evaluated TOE configuration is identical with the delivered product. The TOE consists of the Sagem Identification EAC ePassport application installed on NXP SmartMX J3A080 Revision 2 secure smartcard platform. For contact-less communication with the TOE over the ISO14443A interface an Omnikey CardMan 5321 PC/SC RFID reader was used for the tests. Two different automated test suites were used as test platforms for TOE functional testing and TOE conformity testing to the official ePassport standards.

7.1 Developer's Test according to ATE_FUN

Testing was performed on the final TOE, consisting of the platform and the EAC applet, accessed through a contact-less card reader. All developer tests address the observable behaviour of the TOE. Some tests were performed by design and source code analysis, partially to verify fulfilment of the requirements of the underlying platform to the application.

The scenarios for performing the functional tests with the test tools were structured according to the TOE life cycle phases Manufacturing, Pre-Personalization, Personalization and Operational and including the configurations of Basic Access Control, Active Authentication, Chip Authentication, and Terminal Authentication, added by other test cases, like destructive tests, negative tests, and conformity tests. The test scenarios also include tests for the correct implementation of the e-Passport Chip Application Protocol, the presence and validity of data in the chip, the correctness of cryptographic certificates, and the consistency between data on the card and in the chip. The tests

related to Pre-Personalization, Personalization and Operational 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 allowes 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 developer test results demonstrate that the TSF perform as specified.

7.2 Independent Testing 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

- 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,
- Penetration testing.

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. Within these activities all aspects of the security architecture which were not covered by functional testing were considered.

The implementation of the requirements of the platform ETR and guidance as well as of the security mechanisms of the applet in general was verified by the evaluators. Further aspects were covered by additional tests. 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.

Among other tests, LFI and DFA, perturbation attacks, bypass authentication or access control and exploitation of test features, changing predefined component invocation sequences, using components in unexpected contexts or for unexpected purposes, command execution without secure channel or with bad or missing MAC, resources limit and value range tests, integrity fault and interception event tests, LFI Tests on the ECDSA signature verification method, and time response tests for tracebility attacks were included in the penetration test effort.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential High was successful in the TOE's operational environment as defined in the security target [6] and [8] when all measures required by the developer are applied.

8 Evaluated Configuration

This certification covers the following configuration (or components) of the TOE:

The NXP J3A080 Secure Smartcard Controller Revision 2 (also named JCOP v2.4.1), comprising of (a) the circuitry of the MRTD chip (the NXP P5CD080V0B integrated circuit) with hardware for the contact-less interface; (b) the IC Dedicated Software with the parts IC Dedicated Test Software and IC Dedicated Support Software; (c) the IC Embedded Software (operating system) JCOP v2.4.1 Revision 2;

The MRTD application: Sagem Identification EAC ePassport Applet version 1.2.0;

The associated guidance documentation.

Only the MRTD application is present on the IC.

During Personalization phase the TOE can be identified in two steps. The steps are explained, and the necessary values are given in [11], chapter 2.1:

Step 1: Perform JCOP Product Identification with EAC ePassport Applet in ROM. The JCOP Product Identification is a mandatory step and shall be performed by issuing the IDENTIFY APDU command. The result has to be compared with the value given in [11], chapter 2.1. In order to identify both JCOP and the EAC ePassport Applet module in ROM the IDENTIFY response bytes must be verified against the specified values in [11], chapter 2.1.

Step 2: Perform Sagem Applet Product Identification. The applet instance identification is accomplished by selecting the EAC ePassport Applet and sending a dedicated GET INFO VERSION APDU to the applet instance. The GET INFO VERSION APDU is available in both plain and secure messaging communication mode. The response bytes contain the

Sagem unique configuration item number and version of the EAC ePassport Applet. The values shall be verified against the values specified in [11], chapter 2.1. The EAC ePassport Applet CI-number is 8158-8100-0308. The Sagem EAC Applet version number has the value 00.06.07.0198. For details see [11], chapter 2.1.

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 EAL4 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product [4] (AIS 34).

The following Scheme documents specific for the technology was used:

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

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

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

- All components of the EAL 4+ package as defined in the CC (see also part C of this report)
- The components ALC_DVS.2 and AVA_VAN.5, augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Machine Readable Travel Document with "ICAO Application", Extended Access Control, BSI-PP-0026 [7]
- for the Functionality: PP conformant, Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant, EAL 4 augmented by ALC_DVS.2 and AVA_VAN.5

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

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

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.CF 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 Function	Standard of Implementation	Standard of Application
Triple DES in CBC mode	112	key generation / key derivation	SF.CF.6	-	TR-03110 [17] ICAO Doc 9303 [16]
ECDH Key Agreement Algorithm with EC over GF(p) and 3DES	224 / 256 (for EC) 112 (for 3DES)	key generation / key derivation	SF.CF.4	ANSI X9.63 / ISO 15946-3	TR-03110 [17] TR-03111 [19]
Triple DES in CBC mode	112	encryption / decryption	SF.CF.1	FIPS 46-3	TR-03110 [17] ICAO Doc 9303 [16]
SHA-1	-	document basic access key Derivation / RSA signature generation / chip authentication	SF.CF.2	FIPS 180-2	TR-03110 [17] ICAO Doc 9303 [16]
SHA-224	-	terminal authentication	SF.CF.2	FIPS 180-2	TR-03110 [17]
SHA-256	-	terminal authentication	SF.CF.2	FIPS 180-2	TR-03110 [17]
ECDSA Signature verification	224 / 256	terminal authentication	SF.CF.3	ISO 15946-2	TR-03110 [17] ICAO Doc 9303 [16]
Retail MAC	112	secure messaging - MAC used by SF.SM.1 and SF.SM.2.	SF.CF.1	ISO 9797 (MAC algorithm 3, block cipher DES, Sequence Message Counter, padding mode 2)	-
RSA Digital signature generation	1280 / 1536 / 1792	active authentication	SF.CF.7	ISO 9796-2	TR-03110 [17] ICAO Doc 9303 [16]
Random Number Generation according to class K3, of AIS 20 with SOF-High [4]	-	used for basic access control authentication (SF.I&A.1), terminal authentication (SF.I&A.3), and personalization agent authentication (SF.I&A.4)	SF.CF.8	AIS 20	-

Table 3: Cryptographic Algorithms used by the TOE

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,

[17], 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 3 are implemented by the TOE because of the standards building the TOE application (e.g. TR-03110 [17]). A validity period of each algorithm is not mentioned in BSI-TR-03110 [17]. 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 or she should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

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

APDU Application Protocol Data Unit

API application programming interface

BAC Basic Access Control

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

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

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Common Methodology for Information Technology Security Evaluation

CI-number Configuration Item number

DES Data Encryption Standard; symmetric block cipher algorithm

DOC Document

EAL Evaluation Assurance Level

EC Elliptic Curve

EEPROM Electronically Erasable Programmable Read Only Memory

ES Embedded Software

ETR	Evaluation Technical Report
IC	Integrated Circuit
ICAO	International Civil Aviation Organisation
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility
LDS	Logical Data Structure
MRTD	Machine Readable Travel Document
PP	Protection Profile
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
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 Functions

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 for the Sagem Identification EAC ePassport 1.2.0, Sagem Identification bv, version: 2.0.3, Date 2010-09-10, (confidential document)

[7] Protection Profile: Machine Readable Travel Document with „ICAO Application", Extended Access Control, BSI-PP-0026 , version 1.2, 19.11.2007, BSI

[8] Security Target Lite for the Sagem Identification EAC ePassport 1.2.0, Sagem Identification bv, version: 1.0.0, Date: 2010-10-27

[9] Evaluation Technical Report (ETR), version: 4, 03.11.2010, Sagem Identification EAC ePassport 1.2.0 (confidential document)

[10] Configuration List, Scope for the Sagem EAC ePassport, version 1.2.0, version 2.0.3, Date: 2010-09-10, Sagem Identification bv (confidential document)

[11] Preparative Procedures for the Sagem EAC, ePassport, version 1.2.0, document version 2.0.6, 2010-10-12, Sagem Identification bv

[8] specifically

- AIS 20, Version 1, 02 December 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 6, 07 September 2009, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 7, 03 August 2010, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 1, 25 September 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 6, 03 August 2010, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, 03 September 2009, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 2, 12 November 2007, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[12] Operational User Guidance for the Sagem EAC ePassport, version 1.2.0, document version 2.0.2, 2010-09-10, Sagem Identification bv

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

[14] Certification Report BSI-DSZ-CC-0417-2008 for NXP Smart Card Controller P5CD080V0B with IC dedicated software: Secured Crypto Library Release 2.0 from NXP Semiconductors Germany GmbH, BSI, 13. June 2008, in conjunction with all Assurance Continuity Maintenance Reports, Bundesamt für Sicherheit in der Informationstechnik BSI

[15] Certification Report BSI-DSZ-CC-0597-2010 for NXP J3A080 and J2A080 Secure Smart Card Controller Revision 2 (JCOP v2.4.1) from NXP Semiconductors, 29.10.2010, Bundesamt für Sicherheit in der Informationstechnik BSI (confidential document)

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

[17] Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), TR-03110, version 1.11, 21.02.2008, BSI

[18] ETR for Composition: NXP J3A080 and J2A080 Secure Smart Card Controller Revision 2, version 8, 27.10.2010, TÜVIT GmbH (confidential document)

[19] Technical Guideline: Elliptic Curve Cryptography TR-03111, version 1.11, 17.04.2009, BSI

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.

Annex B: Evaluation results regarding development and production environment

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0643-2010

Evaluation results regarding development and production environment

The IT product Sagem Identification EAC ePassport, Version 1.2.0 (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 4 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 04 November 2010, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.4, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.1)

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

(a) Sagem Identification, Oudeweg 32, 2031 CC Haarlem, The Netherlands (development, manufacturing)

(b) HID Aontec Teoranta, Pairc Tionscail na Tulaigh, Baile na Abhann, Co., Galway, Ireland (inlay manufacturing)

(c) PAV Card, Hamburger Strasse 6, D-22952 Lütjensee, Germany (inlay manufacturing)

For development and production sites regarding the platforms please refer to the certification reports BSI-DSZ-CC-0410-2007, BSI-DSZ-CC-0417-2008, BSI-DSZ-CC-0597-2010 [13, 14, 15].

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

This page is intentionally left blank.