Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0645-2010

for

NXP Secure PKI Smart Card Controllers P5CD145V0A, MSO; P5CC145V0A, MSO; P5CD128V0A, MSO and P5CC128V0A, MSO; each including IC Dedicated Software

from

NXP Semiconductors Germany GmbH

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

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0645-2010

NXP Secure PKI Smart Card Controllers P5CD145V0A, MSO; P5CC145V0A, MSO; P5CD128V0A, MSO and P5CC128V0A, MSO; each including IC Dedicated Software

from	NXP Semiconductors Germany GmbH
PP Conformance:	Security IC Platform Protection Profile, Version 1.0, 23 August 2007, BSI-CC-PP-0035-2007
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ALC_DVS.2, AVA_VAN.5 and ASE_TSS.2

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, 23 July 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 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

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

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

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

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

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

2.2 International Recognition of CC – Certificates (CCRA)

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

As of January 2009 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement.

This evaluation contains the components ALC_DVS.2, AVA_VAN.5 and ASE_TSS.2 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 NXP Secure PKI Smart Card Controllers P5CD145V0A, MSO; P5CC145V0A, MSO; P5CD128V0A, MSO and P5CC128V0A, MSO; each including IC Dedicated Software has undergone the certification procedure at BSI.

The evaluation of the product NXP Secure PKI Smart Card Controllers P5CD145V0A, MSO; P5CC145V0A, MSO; P5CD128V0A, MSO and P5CC128V0A, MSO; each including IC Dedicated Software was conducted by T-Systems GEI GmbH. The evaluation was

completed on 16 July 2010. The T-Systems GEI GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

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

The product was developed by: NXP Semiconductors Germany GmbH.

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

4 Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- 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 shall 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 NXP Secure PKI Smart Card Controllers P5CD145V0A, MSO; P5CC145V0A, MSO; P5CD128V0A, MSO and P5CC128V0A, MSO; each including IC Dedicated Software 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.

[6] Information Technology Security Evaluation Facility

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] NXP Semiconductors Germany GmbH
Georg-Heyken-Str. 1
21147 Hamburg

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 NXP Secure PKI Smart Card Controllers P5CD145V0A, MSO; P5CC145V0A, MSO; P5CD128V0A, MSO and P5CC128V0A, MSO; each including IC Dedicated Software. In short form the TOE is named "NXP Secure Smart Card Controllers P5Cx128V0A/P5Cx145V0A, MSO", in which the optional character x can be replaced by "C" or "D" depending on the configured interfaces. "C" means contact interface only and "D" means dual interface supporting the contact interface and the contactless interface. The "MSO" stands for the IC Dedicated Software, which here is the same for all controllers. The TOE provides a hardware platform for a smartcard operating system. For more details please refer to the block diagram for the TOE in [6] resp. [9], figure 1.

The device is developed for high-end safeguarded applications, and is designed for embedding into chip cards according to ISO/IEC 7816 and for contactless applications. Usually a Security IC (e.g. a smartcard) is assigned to a single individual only, but it may also be used by multiple applications in a multi-provider environment. Therefore the TOE might store and process secrets of several applications, which must be protected from each other in order to meet security requirements for each single security module. Secret data shall be used as input for calculation of authentication data, calculation of signatures and encryption of data and keys.

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Security IC Platform Protection Profile, Version 1.0, 23 August 2007, BSI-CC-PP-0035-2007 [10].

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, AVA_VAN.5 and ASE_TSS.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] resp. [9], 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 Features:

TOE Security Features	Addressed issue
SS.RNG	Random Number Generator
SS.HW_DES	Triple-DES coprocessor
SS.HW_AES	AES coprocessor
SF.OPC	Control of Operating Conditions
SF.PHY	Protection against Physical Manipulation
SF.LOG	Logical Protection
SF.COMP	Protection of the Mode Control
SF.MEM_ACC	Memory Access Control
SF.SFR_ACC	Special Function Register Access Control

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] resp. [9], chapter 8.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. 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], chapter 3.2, 3.3 and 3.4.

This certification covers the following configurations of the TOE: Four major configurations are present, which are denoted by names P5CD128V0A, P5CD145V0A, P5CC128V0A, and P5CC145V0A. All of them use the same hardware chip including 144 kBytes of EEPROM and both, the ISO/IEC 7816 contact interface and the ISO/IEC 14443 contactless interface, but differently configured (see table 3 below).

More details con be found in the Security Target [6] resp. [9], chapter 1.4 (in particular chapter 1.4.1.1 and 1.4.2.1).

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:

NXP Secure PKI Smart Card Controllers P5CD145V0A, MSO; P5CC145V0A, MSO; P5CD128V0A, MSO and P5CC128V0A, MSO; each including IC Dedicated Software

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Date	Form of Delivery
1	HW	NXP Secure Smart Card Controller P5CD145V0A	V0A	T051A_20090820.gds2	Wafer, module, inlay package (dice have nameplate: T051A)
	HW	NXP Secure Smart Card Controller P5CC145V0A	V0A	T051A_20090820.gds2	Wafer, module, package (dice have nameplate: T051A)
	HW	NXP Secure Smart Card Controller P5CD128V0A	V0A	T051A_20090820.gds2	Wafer, module, inlay package (dice have nameplate: T051A)

	HW	NXP Secure Smart Card Controller P5CC128V0A	V0A	T051A_20090820.gds2	Wafer, module package (dice have nameplate: T051A)
2	SW	Test ROM Software (the IC Dedicated Test Software)	Version 97	09.12.2009	Test-ROM on the chip acc. to tmfos_97_collected.ms3
3	SW	Boot ROM Software (part of the IC Dedicated Support Software)	Version 97	09.12.2009	Test-ROM on the chip acc. to tmfos_97_collected.ms3
4	SW	MIFARE Operating System (part of the IC Dedicated Support Software)	Version 97	09.12.2009	Test-ROM on the chip acc. to tmfos_97_collected.ms3
5	Doc	Data Sheet P5Cx128/P5Cx145 family, Secure dual interface and contact PKI smart card controller [12]	Rev. 3.0	08.06.2010	Document Number: 177930
6	Doc	Instruction Set, SmartMX-Family [13]	Revision 1.1,	04.07.2006	Document Number: 084111
7	Doc	Guidance, Delivery and Operation Manual NXP Secure Smart Card Controllers, P5Cx128V0A/ P5Cx145V0A, MSO [14]	Version 1.2	18.06.2010	Document Number: 185112

Table 2: Deliverables of the TOE

The hardware part of the TOE is identified by P5CD145V0A, P5CC145V0A, P5CD128V0A, P5CC128V0A and a so-called nameplate (on-chip identifier) is coded in a metal mask onto the chip during production and can be checked by the customer. The nameplate "T051A" is specific for the SSMC (Singapore) production as outlined in the guidance documentation [14]. This nameplate identifies Version V0A of the hardware, but does not identify specifically the TOE configurations. For identification of a specific configuration, the device coding bytes stored in the EEPROM can be used (see [12] chapter 11.6). More details about the device coding bytes can be found in the chapter 8.

For details on evaluated package types see Security Target [6] resp. [9], chapter 1.4.1.3

Items 2, 3 and 4 in table 2 are not delivered as single pieces, but included in the Test ROM part of the chip. They are identified by their unique version numbers.

The delivery process from NXP to their customers (to phase 4 or phase 5 of the life cycle) guarantees that the customer is aware of the exact versions of the different parts of the TOE as outlined above.

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues: Symmetric cryptographic block cipher algorithms (Triple-DES and AES), to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols and it will provide a random number generation of appropriate quality. The Triple-DES coprocessor supports single DES and Triple-DES operations. Only Triple-DES is used in this evaluation, in 2-key or 3-key operation. The AES coprocessor supports AES operation with three different key lengths of 128, 192 or 256 bit. The FameXE coprocessor supplies basic arithmetic functions to support implementation of asymmetric cryptographic algorithms by the Security IC Embedded Software. The random generator provides true random numbers without pseudo random calculation.

As the TOE is a hardware security platform, the security policy of the TOE provides countermeasures against: leakage of information, physical probing, malfunctions, physical manipulations, access to code, access to data memory, abuse of functionality.

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:

Protection during Packaging, Finishing and Personalization, Usage of Hardware Platform, Treatment of User Data, Check of initialisation data by the Smart Card Embedded Software, Usage of Key-dependent Functions. Details can be found in the Security Target [6], chapter 3 and in the Protection Profile BSI-CC-PP-0035-2007 [10].

5 Architectural Information

The NXP Secure PKI Smart Card Controllers P5CD145V0A, MSO; P5CC145V0A, MSO; P5CD128V0A, MSO and P5CC128V0A, MSO; each including IC Dedicated Software is an integrated circuit (IC) providing a hardware platform for a Security IC Embedded Software. A top level block diagram and a list of subsystems can be found within the TOE description of the [6] resp. [9]. The complete hardware description and the complete instruction set of these Smart Card Controllers can be found in the Data Sheet [12] and Instruction Set [13].

The hardware platform comprises the following components: 8-bit CPU, Special Function Registers, Triple-DES Co-Processor, AES co-processor, FameXE Co-Processor, Random Number Generator (RNG), Power Module and a module comprising Security Sensors and Filters. In addition the hardware platform comprises a contact-based interface and a contactless interface. The CPU is equipped with a Memory Management Unit and provides three different CPU Modes in order to separate different applications running on the TOE. More details about the CPU Modes can be found in [6] resp. [9], chapter 1.4.2.1.

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 tests performed by the developer were divided into six categories:

1. technology development tests as the earliest tests to check the technology against the specification and to get the technology parameters used in simulations of the circuitry (this testing is not strictly related to Security Functionalities);
2. tests which are performed in a simulation environment with different tools for the analogue circuitries and for the digital parts of the TOE;
3. regression tests of the hardware within a simulation environment based on special software dedicated only for the regression tests;
4. regression tests which are performed for the IC Dedicated Test Software and for the IC Dedicated Support Software on emulator versions of the TOE and within a software simulation of chip in special hardware;
5. characterisation and verification tests to release the TOE to production:

   - used to determine the behaviour of the chip with respect to different operating conditions and varied process parameters (often also referred to as characterisation tests)

   - special verification tests for Security Functionalities which were done with samples of the TOE (referred also as developers security evaluation) and which include also layout tests by automatic means and optical control, in order to verify statements concerning the layout;

6. functional production tests, which are done for every chip to check its correct functionality as a last step of the production process (phase 3).

The developer tests cover all Security Functionalities and all security mechanisms as identified in the functional specification.

The evaluators were able to repeat the tests of the developer either using the library of programs, tools and prepared chip samples delivered to the evaluator or at the developers site. They performed independent tests to supplement, augment and to verify the tests performed by the developer. The tests of the developer were repeated by sampling, by repetition of complete regression tests and by software routines developed by the evaluators and computed on samples with evaluation operating system. For the developer tests repeated by the evaluators other test parameters were used and the test equipment was varied. Security features of the TOE realised by specific design and layout measures were checked by the evaluators during layout inspections both in design data and on the final product.

The evaluation provides evidence that the actual version of the TOE provides the Security Functionalities as specified by the developer. The test results confirm the correct implementation of the TOE Security Functionalities.

For penetration testing the evaluators took all Security Functionalities into consideration. Intensive penetration testing was planned based on the analysis results and performed for the underlying mechanisms of Security Functionalities using bespoke equipment and

expert know how. The penetration tests considered both the physical tampering of the TOE and attacks which do not modify the TOE physically.

8 Evaluated Configuration

The evaluated NXP Secure Smart Card Controllers can be delivered in different configurations. All major configurations listed in the following table are covered by the evaluation. Due to the naming conventions of the MX family the configured TOEs have different names.

	P5CD145V0A, MSO	**P5CC145V0A, MSO**	**P5CD128V0A, MSO**	**P5CC128V0A, MSO**
Contact-less interface	available	not available	available	not available
Mifare OS	available	not available	available	not available
accessible EEPROM	144kByte	144kByte	128kByte	128kByte
Device coding byte	21 17 4B	11 17 4A	21 17 49	11 17 48

Table 3:Overview of major configurations

The NXP Secure Smart Card Controllers P5Cx128V0A/P5Cx145V0A, MSO hardware platform was tested including all major configurations as well as all minor configuration options that can be selected based on table 2 in section 1.4.1.2 of [6]. All major and minor configurations are available to the evaluator. Beside the differences listed in table 4 there are no other differences between the major configurations (note that the Mifare OS is only available for the configurations with contact-less interface). The major configuration does not have dependencies to security features. All minor configuration options that are part of the evaluation were tested. The minor configuration options behave as specified and described in [12] and [14]. Therefore the results described in this document are applicable for the major configurations P5CD145V0A, MSO, P5CC145V0A, MSO, P5CD128V0A, MSO and the P5CC128V0A, MSO as well as for all minor configurations described in [6].

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 (see [4] (AIS 34)] and guidance specific for the technology of the product.

The following guidance specific for the technology was used:

(i) The Application of CC to Integrated Circuits

(ii) Application of Attack Potential to Smartcards

(see [4], AIS 25, AIS 26).

For the RNG assessment the scheme interpretations AIS 31 was used (see [4]).

To support composite evaluations according to AIS 36 the document ETR for composite evaluation [11] was provided and approved. This document provides details of this platform evaluation that have to be considered in the course of a composite evaluation on top.

The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

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, AVA_VAN.5 and ASE_TSS.2 augmented for this TOE evaluation.

The evaluation has confirmed:

- PP Conformance: Security IC Platform Protection Profile, Version 1.0, 23 August 2007, BSI-CC-PP-0035-2007 [10]
- for the Functionality: PP conformant plus product specific extensions Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant EAL 5 augmented by ALC_DVS.2, AVA_VAN.5 and ASE_TSS.2

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 4, Para. 3, Clause 2). This holds for:

- the TOE Security Functionality SS.HW_DES for Triple-DES and
- the TOE Security Functionality SS.HW_AES for AES

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

The Cryptographic Functionalities: 2-key Triple DES (2TDES) provided by the TOE achieves a security level of maximum 80 Bits (in general context).

10 Obligations and Notes for the Usage of the TOE

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

aspects of assumptions, threats and policies as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

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

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

Some security measures are partly implemented in the hardware and require additional configuration or control or measures to be implemented by the IC Dedicated Support Software or Embedded Software.

For this reason the TOE includes guidance documentation (see table 2) which contains guidelines for the developer of the IC Dedicated Support Software and Embedded Software on how to securely use the microcontroller chip and which measures have to be implemented in the software in order to fulfil the security requirements of the Security Target of the TOE.

In the course of the evaluation of the composite product or system it must be examined if the required measures have been correct and effectively implemented by the software. Additionally, the evaluation of the composite product or system must also consider the evaluation results as outlined in the document ETR for composite evaluation [11].

In addition, the following aspects need to be fulfilled when using the TOE:

The guidance documentation [12], [13] and [14] contain all necessary information about the usage of the TOE by the Security IC Embedded Software developer (in the context of this evaluation Security IC Embedded Software is a term used for all software in the Application-ROM of the TOE, including operating systems).

Especially the advice for the developer, which measures he has to implement in the software in order to fulfil the security requirements of the Security Target for the environment of the TOE, is contained in the user guide [14]. This means that in the course of the evaluation of the product or system it should be examined, if the requirements defined in [14] are fulfilled by the application developer in order to assure that the TOE is used in its evaluated form.

As an additional check it needs to be examined if the assumptions on the environment defined in the Security Target [6] resp. [9] for the smartcard lifecycle phase(s) covered by the developer of the respective product are fulfilled. Note, however, that these assumptions are either

- fulfilled by the Security IC Embedded Software, and in this case their fulfilment is already covered by the fulfilment of the requirements in the user guidance as described above, or
- fulfilled by the development environment of the Embedded Software developer of the respective product, i.e. those measures which fulfil the general requirements of CC for the development environment defined by the aspect ALC.

This implies that the examination of the assumptions in the Security Target [6] resp. [9] can be reduced to a mapping to examinations already done for the sets of requirements mentioned above. If these examinations come up with a positive result, the security

functionality provided by the TOE according to the Security Target [6] resp. [9] can be assumed to be effective.

The following result from the evaluation of the Aspect ALC_DVS Development Security can be useful for further evaluations: The examination of the procedures used by NXP, BL ID to introduce the Security IC Embedded Software into the ROM mask of the chip has shown: The procedures are suitable to assure that the correct version of the Security IC Embedded Software (i. e. that version transmitted to NXP, BL ID by the application developer) is contained in the chip delivered by NXP, BL ID.

The following result from the evaluation of the aspect AGD resp. ALC_CMC and ALC_CMS can be useful for further evaluations: The Fabkey procedure (see the developer documentation for the description) is handled by NXP, BL ID in a way which allows introducing individual cryptographic keys in each individual TOE. Confidentiality and integrity of these keys are protected in this procedure. Therefore this key can be used as a means for mutual cryptographic authentication between the TOE and the system of the card manufacturer. This may be used to protect sensitive functions of the Security IC Embedded Software (e. g. personalisation functions) against unauthorised use.

11 Security Target

For the purpose of publishing, the Security Target [9] 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

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

CPU Central Processing Unit

DES Data Encryption Standard; symmetric block cipher algorithm

DPA Differential Power Analysis

EAL Evaluation Assurance Level

EEPROM Electrically Erasable Programmable Read Only Memory

ETR Evaluation Technical Report

IC Integrated Circuit

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

MMU Memory Management Unit

MSO	Mifare Simulataneous Operation: Indicator for the IC Dedicated Software including the Mifare Operating System
OTP	One Time Programmable (a certain part of the EEPROM)
PP	Protection Profile
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read Only Memory
SF	Security Function
SFP	Security Function Policy
SS	Security Services
ST	Security Target
TOE	Target of Evaluation
Triple-DES	Symmetric block cipher algorithm based on the DES
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy
TSS	TOE Summary Specification
UART	Universal Asynchronus Receiver and Transmitter

12.2 Glossary

Augmentation - The addition of one or more requirement(s) to a package.

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

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

Informal - Expressed in natural language.

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

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

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

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

TOE Security Functionality - combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

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

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

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

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

[6] Security Target P5Cx128V0A/P5Cx145V0A, MSO, NXP Secure Smart Card Controllers, NXP Semiconductors, Business Line Identification, Version 1.6, June 7th, 2010 (confidential document)

[7] Evaluation Technical Report, V. 1.1, 15th July 2010, BSI-DSZ-CC-0645, NXP Secure PKI Smart Card Controllers P5CD145V0A, MSO; P5CC145V0A, MSO; P5CD128V0A, MSO; P5CC128V0A, MSO, each including IC Dedicated Software (confidential document)

[8] Configuration List for the P5Cx128V0A/P5Cx145V0A, MSO, Rev. 1.2, NXP Semiconductors, 07.07.2010

[9] Security Target Lite BSI-DSZ-0645, Version 1.6, 07 June 2010, P5Cx128V0A/P5Cx145V0A, MSO NXP Smart Card Controllers, NXP Semiconductors (sanitised public document)

[8] specifically

- AIS 20, Version 1, 2. December 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 6, 7 September 2009, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 6, 07 May 2009, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 1, 25 Sept. 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 5, 17 May 2010, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, 3 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

[10] Security IC Platform Protection Profile, Version 1.0, 15.06.2007, registered and certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under reference BSI-CC-PP-0035

[11] ETR for composition according to AIS 36 for the Product NXP P5Cx128V0A/P5Cx145V0A, MSO Secure Smart Card Controller, Version 1.1, 15th July 2010, BSI-DSZ-CC-0645, T-Systems GEI GmbH (confidential document)

[12] Data Sheet P5Cx128/P5Cx145 family, Secure dual interface and contact PKI smart card controller, NXP Semiconductors, Rev. 3.0, Document Number 177930, 8 June 2010

[13] Instruction Set, SmartMX-Family, Secure and PKI Smart Card Controller, Philips Semiconductors, Revision 1.1, Document Number: 084111, July 04, 2006

[14] Guidance, Delivery and Operation Manual NXP Secure Smart Card Controllers P5Cx128V0A/P5Cx145V0A, MSO, NXP Semiconductors, Business Line identification, Rev. 1.2, Document Number 185112, 18 June 2010

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance Claim (Release 3, 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 37

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0645-2010

Evaluation results regarding development and production environment

The IT product NXP Secure PKI Smart Card Controllers P5CD145V0A, MSO; P5CC145V0A, MSO; P5CD128V0A, MSO and P5CC128V0A, MSO; each including IC Dedicated Software (Target of Evaluation, TOE) has been evaluated at an accredited and 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 23 July 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.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:

1. NXP Semiconductors Germany GmbH, Business Line Identification, Georg-Heyken-Str. 1, D-21147 Hamburg (Development Center)
2. NXP Semiconductors GmbH, Document Control Office, Mikron-Weg 1, A-8101 Gratkorn (Documentation)
3. NXP Semiconductors (Thailand), Assembly Plant Bangkok, Thailand (APB), 303 Moo 3 Chaengwattana Rd., Laksi, Bangkok 10210 Thailand (Assembly, Test and Delivery)
4. NXP Semiconductors Germany GmbH, IC Manufacturing Operations - Test Center Hamburg (IMO TeCH), Stresemannallee 101, D-22529 Hamburg (Test and Delivery)
5. Systems on Silicon Manufacturing Co. Pte. Ltd. (SSMC), 70 Pasir Ris Drive 1, Singapore 519527, Singapore (Semiconductor Factory)
6. Toppan Photomasks Korea Ltd., 345-1, Sooha-Ri ShinDoon-Myon, 467-840 Ichon, South Korea (Mask Shop)
7. Chipbond Technology Corporation, No. 3, Li-Hsin Rd. V, Science Based Industrial Park, Hsin-Chu City, Taiwan R.O.C. (Wafer Bumping)
8. NedCard B.V., Bijsterhuizen 25-29, 6604 LM Wijchen, The Netherlands (Module Assembly)
9. HID Global Ireland, Paic Tionscail na Tulaigh, Balle na hAbhann, Co. Galway, Ireland (Inlay Assembly)
10. Smartrac Technology GmbH, Wernerwerkstr. 2, 93049 Regensburg, Germany (Inlay assembly)
11. Smartrac Technology Ltd., 142 Moo, Hi-Tech Industrial Estate, Tambon Ban Laean, Amphor Bang-Pa-In, 13160 Ayutthaya, Thailand (Inlay assembly)

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