Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0858-2013

for

NXP Secure PKI Smart Card Controllers P5CD128V0v/ V0B(s), P5CC128V0v/ V0B(s), P5CD145V0v/ V0B(s), P5CC145V0v/ V0B(s), P5CN145V0v/V0B(s), each including IC Dedicated Software

from

NXP Semiconductors Germany GmbH

Deutsches IT-Sicherheitszertifikat
erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0858-2013

Smart Card Controller

NXP Secure PKI Smart Card Controllers P5CD128V0v/ V0B(s), P5CC128V0v/ V0B(s), P5CD145V0v/ V0B(s), P5CC145V0v/ V0B(s), P5CN145V0v/V0B(s), each including IC Dedicated Software

from	NXP Semiconductors Germany GmbH
PP Conformance:	Security IC Platform Protection Profile, Version 1.0, 15 June 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 ASE_TSS.2, AVA_VAN.5 and ALC_DVS.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 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 12 June 2013
For the Federal Office for Information Security

SOGIS
IT SECURITY CERTIFIED

Bernd Kowalski   L.S.
Head of Department

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

---

[1]   Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

Contents

A   Certification

1   Specifications of the Certification Procedure

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

- BSIG[2]

- BSI Certification Ordinance[3]

- BSI Schedule of Costs[4]

- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)

- DIN EN 45011 standard

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

- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]

- Common Methodology for IT Security Evaluation, Version 3.1 [2]

- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

2   Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1   European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and in addition at higher recognition levels for IT-Products related to certain technical domains only.

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

---

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

3   Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

4   Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5   Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

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

2.2 International Recognition of CC – Certificates (CCRA)

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

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

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

This evaluation contains the components ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, ASE_TSS.2, ATE_DPT.3 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 NXP Secure PKI Smart Card Controllers P5CD128V0v/ V0B(s), P5CC128V0v/ V0B(s), P5CD145V0v/ V0B(s), P5CC145V0v/ V0B(s), P5CN145V0v/V0B(s), each including IC Dedicated Software has undergone the certification procedure at BSI. The suffix "v" in the version information indicates the hardware platform subrevision of the TOE, which can be either "A" or "B". This is a re-certification based on BSI-DSZ-CC-0645-2010. Specific results from the evaluation process BSI-DSZ-CC-0645-2010 were re-used.

The evaluation of the product NXP Secure PKI Smart Card Controllers P5CD128V0v/ V0B(s), P5CC128V0v/ V0B(s), P5CD145V0v/ V0B(s), P5CC145V0v/ V0B(s), P5CN145V0v/V0B(s), each including IC Dedicated Software, was conducted by T-Systems GEI GmbH. The evaluation was completed on 13 May 2013. 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.

---

[6]   Information Technology Security Evaluation Facility

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

4   Validity of the Certification Result

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

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

5   Publication

The product NXP Secure PKI Smart Card Controllers P5CD128V0v/ V0B(s), P5CC128V0v/ V0B(s), P5CD145V0v/ V0B(s), P5CC145V0v/ V0B(s), P5CN145V0v/V0B(s), each including IC Dedicated Software has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

---

[7]   NXP Semiconductors Germany GmbH
       Stresemannallee 101
       22529 Hamburg

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 NXP Secure PKI Smart Card Controllers P5CD128V0v/ V0B(s), P5CC128V0v/ V0B(s), P5CD145V0v/ V0B(s), P5CC145V0v/ V0B(s), P5CN145V0v/ V0B(s), each including IC Dedicated Software provide a hardware platform for the implementation of a smart card operating systems including multiple applications. The hardware platform provides coprocessors for cryptographic algorithms Triple-DES with up to three keys and AES with different key lengths as well as a coprocessor for large integer arithmetic operations. In addition the hardware platform includes a True Random Number Generator suitable to generate cryptographic keys. The TOE supports the ISO/IEC 7816 contact interface with UART and the ISO/IEC 14443 A contactless interface. The contactless interface together with IO3 can be configured in S^2C mode to support Near Field Communication (NFC). The implementation of multiple applications is supported by the CPU offering different CPU modes with gradual permissions and memory management control supporting the separation of different memory segments. The MIFARE FleX or MIFARE MSO as part of the IC Dedicated Software does not contribute to security mechanisms of the devices and was not subject of the evaluation.

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, 15 June 2007, BSI-CC-PP-0035-2007 [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 5 augmented by ASE_TSS.2, AVA_VAN.5 and ALC_DVS.2.

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 Functionality	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 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] and [8], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6] and [8], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of

Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [8], chapter 3.2 and 3.3.

This certification covers several configurations of the TOE. For details refer to chapter 8.

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 P5CD128V0v/ V0B(s), P5CC128V0v/ V0B(s), P5CD145V0v/ V0B(s), P5CC145V0v/ V0B(s), P5CN145V0v/V0B(s), each including IC Dedicated Software

where "v" is either "A" or "B".

The following table outlines the TOE deliverables:

The subsequent information is taken from the ST, the first part covers the TOE version V0A with MIFARE MSO as initially evaluated. The second part includes the TOE version V0A with MIFARE FleX, the next two cover the version V0B with MIFARE FLeX option from the two wafer . Note, that the MSO variation is not offered for the version V0B of the TOE.

TOE deliverables for the TOE version V0A with MIFARE MSO
NXP Secure Smart Card Controllers P5Cx128/P5Cx145V0A Release V0A (GDS 2 File: T051A_20090820.gds2) in form of wafer, modules and packages. The dice include reference T051A.
Test ROM Software for MIFARE MSO (part of the IC Dedicated Test Software) Version 97, December 9th, 2009, Test ROM on the chip (tmfos_97_collected.ms3)
Boot ROM Software for MIFARE MSO (part of the IC Dedicated Support Software) Version 97, December 9th, 2009, Test ROM on the chip (tmfos_97_collected.ms3)
MIFARE Operating System MSO (part of the IC Dedicated Support Software) thVersion 97, December 9 , 2009, Test ROM on the chip (tmfos_97_collected.ms3)
Data Sheet P5Cx128/P5Cx145 family, Secure dual interface and contact PKI smart card controller, NXP Semiconductors, Rev. 3.5, Document Number 177935, 14 February 2012
Instruction Set, SmartMX-Family, Secure and PKI Smart Card Controller, Philips Semiconductors, Revision 1.1, Document Number: 084111, July 04, 2006
Guidance, Delivery and Operation Manual, NXP Secure Smart Card Controllers P5Cx128/ P5Cx145, NXP Semiconductors, Version 1.7, Document Number: 185117, 19 March 2013

TOE deliverables for the TOE version V0A and MIFARE FLeX
NXP Secure Smart Card Controllers P5Cx128/P5Cx145V0A
Release V0A (GDS 2 File: T051A_20090820.gds2) in form of wafer, modules and packages. The dice include reference T051A.
Test ROM Software for MIFARE FLeX (the IC Dedicated Test Software) Version 102, April 27th, 2011, Test ROM on the chip (tmfos_102_collected.hex)
Boot ROM Software for MIFARE FLeX (part of the IC Dedicated Support Software) Version 102, April 27th, 2011, Test ROM on the chip (tmfos_102_collected.hex)
MIFARE FLeX Operating System (part of the IC Dedicated Support Software) Version 102, April 27th, 2011, Test ROM on the chip (tmfos_102_collected.hex)
Data Sheet P5Cx128/P5Cx145 family, Secure dual interface and contact PKI smart card controller, NXP Semiconductors, Rev. 3.5, Document Number 177935, 14 February 2012
Instruction Set, SmartMX-Family, Secure and PKI Smart Card Controller, Philips Semiconductors, Revision 1.1, Document Number: 084111, July 04, 2006
Guidance, Delivery and Operation Manual, NXP Secure Smart Card Controllers P5Cx128/ P5Cx145, NXP Semiconductors, Version 1.7, Document Number: 185117, 19 March 2013
TOE deliverables for the TOE with release V0B from SSMC with MIFARE FLeX
NXP Secure Smart Card Controllers P5Cx128/P5Cx145V0B Release V0B (GDS 2 File: T051B_20100617_C.gds2) in form of wafer, modules and packages. The dice include reference T051B.
Test ROM Software for MIFARE FLeX (the IC Dedicated Test Software) Version 102, April 27th, 2011, Test ROM on the chip (tmfos_102_collected.hex)
Boot ROM Software for MIFARE FLeX (part of the IC Dedicated Support Software) Version 102, April 27th, 2011, Test ROM on the chip (tmfos_102_collected.hex)
MIFARE FLeX Operating System (part of the IC Dedicated Support Software) Version 102, April 27th, 2011, Test ROM on the chip (tmfos_102_collected.hex)
Data Sheet P5Cx128/P5Cx145 family, Secure dual interface and contact PKI smart card controller, NXP Semiconductors, Rev. 3.5, Document Number 177935, 14 February 2012
Instruction Set, SmartMX-Family, Secure and PKI Smart Card Controller, Philips Semiconductors, Revision 1.1, Document Number: 084111, July 04, 2006
Guidance, Delivery and Operation Manual, NXP Secure Smart Card Controllers P5Cx128/ P5Cx145, NXP Semiconductors, Version 1.7, Document Number: 185117, 19 March 2013
TOE deliverables for the TOE with release V0B from Globalfoundries with MIFARE FLeX
NXP Secure Smart Card Controllers P5Cx128/P5Cx145V0B Release V0B (GDS 2 File: s051B.gds2) in form of wafer, modules and packages. The dice include reference T051B.

Test ROM Software for MIFARE FLeX (the IC Dedicated Test Software) Version 102, April 27th, 2011, Test ROM on the chip (tmfos_102_collected.hex)
Boot ROM Software for MIFARE FLeX (part of the IC Dedicated Support Software) Version 102, April 27th, 2011, Test ROM on the chip (tmfos_102_collected.hex)
MIFARE FLeX Operating System (part of the IC Dedicated Support Software) Version 102, April 27th, 2011, Test ROM on the chip (tmfos_102_collected.hex)
Data Sheet P5Cx128/P5Cx145 family, Secure dual interface and contact PKI smart card controller, NXP Semiconductors, Rev. 3.5, Document Number 177935, 14 February 2012
Instruction Set, SmartMX-Family, Secure and PKI Smart Card Controller, Philips Semiconductors, Revision 1.1, Document Number: 084111, July 04, 2006
Guidance, Delivery and Operation Manual, NXP Secure Smart Card Controllers P5Cx128/ P5Cx145, NXP Semiconductors, Version 1.7, Document Number: 185117, 19 March 2013

Table 2: Deliverables of the TOE

Note that only 4 items (the hardware platform and three documents) are delivered since the IC Dedicated Software included in the ROM is delivered on the chip. There is one Data Sheet and one Guidance, Delivery and Operation Manual for all configurations of the TOE.

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:

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.

Hence the TOE shall:

● maintain the integrity and the confidentiality of data stored in the memory of the TOE and

● maintain the integrity, the correct operation and the confidentiality of Security Functions (security mechanisms and associated functions) provided by the TOE.

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:

Name	Title
A.Process-Sec-IC	Protection during Packaging, Finishing and Personalization
A.Plat-Appl	Usage of Hardware Platform
A.Resp-Appl	Treatment of User Data
A.Check-Init	Check of initialization data by the Security IC Embedded Software

Name	Title
A.Key-Function	Usage of Key-dependent Functions

Details can be found in the Security Target [6] and [8], chapter 3.4.

5 Architectural Information

The hardware platform comprises the following components: 8-bit CPU, Special Function Registers, Triple-DES coprocessor, AES coprocessor, FameXE coprocessor and a Random Number Generator (RNG). Further on the hardware platform implements a contact-based interface and a contactless interface with power module including security sensors and filters. The CPU is equipped with a Memory Management Unit and provides different CPU Modes in order to support the separation of different applications running on the TOE. Security features for physical protection are realized within the layout of the whole circuitry.

The Special Function Registers provide an interface to the TOE security functionality that can be controlled by the Security IC Embedded Software. The NXP Secure Smart Card Controllers P5Cx128/P5Cx145V0v/ V0B(s) provides different levels of access control to the Special Function Register with the different CPU Modes including configurable access control to Special Function Registers for the User Mode and the Mifare Mode. The MIFARE operating system is called via CVEC7 from System Mode, when the implementation is enabled with device configuration B1 or B4, respectively D1 or D4

The FameXE does not provide a cryptographic algorithm itself. The modular arithmetic functions are suitable to implement different asymmetric cryptographic algorithms.

The TOE executes the IC Dedicated Support Software (Boot Software) during the start up to configure and initialise the hardware. This software is executed in the Boot Mode. After the start-up is finished and the CPU Mode changed to System Mode it is not possible to re-enter the Boot Mode without forcing a reset.

The MIFARE Operating System supports the functions to exchange data in the contact-less mode with other MIFARE components. The MIFARE Operating System is executed in the MIFARE Mode to ensure a strict separation between IC Dedicated Support Software and Security IC Embedded Software. Note, that the term MIFARE Operating System as being used in the Security Target refers to both, the MIFARE MSO and the MIFARE FLeX variant available for the TOE. Based on the partitioning of the memories the MIFARE Operating System is not able to access the Security IC Embedded Software and the data stored in the EEPROM area that is not reserved for the MIFARE Operating System. In the same way the access to the program and the data of the MIFARE Operating System is denied for the Security IC Embedded Software. A limited memory area for the data exchange (between Security IC Embedded Software and MIFARE Operating System) can be configured by the Security IC Embedded Software.

The hardware platform comprises a contact based interface and a contactless interface. Both interfaces can be used independent from each other. Depending on the major configuration the contactless interface is disabled, or configured as S^{2}C interface. Based on a specific minor configuration and an associated clock configuration both interfaces could be used simultaneously.

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 can be divided into the following categories:

1. tests which are performed in a simulation environment with different tools for the analogue circuitries and for the digital parts of the TOE;

2. functional tests which are performed with special software

3. characterisation and verification tests to release the hardware platform for production including tests with different operating conditions as well as special verification tests for security services and security features of the hardware

4. functional tests at the end of the production process using IC Dedicated Test Software. These tests are executed for every chip to check its correct functionality as last step of phase 3.

The developer tests cover all TSFIs as identified in the functional specification as well as in the test documentation.

The tests of the evaluators comprise special tests and examination of the hardware platform using open samples. In addition the evaluators perform tests of the hardware platform using different configurations.

For penetration testing the evaluators took all TOE Security Functionality into consideration. Extensive penetration testing was performed to test the security mechanisms used to provide the Security Services and Security Features. The tests for the hardware platform comprise the use of bespoke equipment and expert knowledge. The penetration tests considered both the physical tampering of the hardware platform including information that can be gathered by reverse engineering to support other attacks. Further on attacks that do not modify the hardware platform physically such as side channel analysis for the coprocessors (AES, Triple-DES) and perturbation attacks were performed. The test of the hardware platform comprises attacks that must be averted by the combination of the hardware platform and the Security IC Embedded Software as well as attacks against the hardware platform directly.

8   Evaluated Configuration

This certification covers the following configurations of the TOE:

The NXP Secure Smart Card Controllers P5Cx128/P5Cx145V0v/ V0B(s) can be delivered in different configurations, specifically it is delivered with different MIFARE versions. The term "MIFARE Operating System" denotes the TOE with MIFARE MSO or MIFARE FLeX option according to the ST. All configurations listed in the following table are covered by the evaluation. Due to the naming conventions of the SMX family the configured TOEs have different names.

	P5CD145V0v	**P5CC145V0v**	**P5CD128V0v**	**P5CC128V0v**	**P5CN145V0v**
Contactless	available	not available	available	not available	configured as S2C interface
interface Mifare OS	available	not available	available	not available	not available
accessible EEPROM	144kByte	144kByte	128kByte	128kByte	144kByte

Tabelle 3: Overview of major configurations

The P5CD145V0v/V0v(s) and its major configurations were all tested during the evaluation. All configurations are available to the evaluator. Beside the differences listed in table 3 there are no other differences between the configurations (note that the MIFARE Operating System is only available for the configurations with either contact-less interface or S2C interface). The term "MIFARE Operating System" in this context according to the ST, [6] covers both variants of the chip the MIFARE MSO option and the MIFARE FLeX option. Note, that according to the ST, the MSO option is no longer offered as variant of the TOE. This means that customers providing a new IC Security Embedded Software will get the MIFARE FleX variant. The configuration does not have dependencies to security features. Therefore the results described in this document are also applicable for the P5CD128V0v/V0v(s), P5CC128V0v/V0v(s), P5CD145V0v/V0v(s), P5CC145V0v/V0v(s), and the P5CN145V0v/V0v(s).

9   Results of the Evaluation

9.1   CC specific results

The Evaluation Technical Report (ETR) [9] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used for those components up to EAL5 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

(i)   The Application of CC to Integrated Circuits

(ii)   Application of Attack Potential to Smartcards

(iii)   Guidance, Smartcard Evaluation

(see [4], AIS 25, AIS 25, AIS 37).

For 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 [10] 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.

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

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0645-2010, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was the extension of the life cycle and the re-assessment. The extension of the life cycles includes an additional wafer production site and a new assembly sites. In this context als the verification of the devices from the additional production site as well as up to date side channel analysis as well as fault analysis were part of the re-evaluation.

The evaluation has confirmed:

- PP Conformance: Security IC Platform Protection Profile, Version 1.0, 15 June 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 ASE_TSS.2, AVA_VAN.5 and ALC_DVS.2

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 SS.HW_DES for Triple-DES.

- the TOE Security functionality SS.HW_AES for AES

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

The Cryptographic Functionality 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 documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and

techniques to be covered, he should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

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 correctly 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 [10].

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

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
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
CPU	Central Processing Unit
DES	Data Encryption Standard
EAL	Evaluation Assurance Level
EEPROM	Electrically Erasable Programmable Read Only Memory
ETR	Evaluation Technical Report
IC	Integrated Circuit
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITSEF	Information Technology Security Evaluation Facility

NFC	Near Field Communication
PKI	Public Key Infrastructure
PP	Protection Profile
RNG	Random Number Generator
ROM	Read Only Memory
S2C	Smart card interface standard complying with ISO/IEC 18092
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
UART	Universal Asynchronous Receiver 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 BSI-DSZ-CC-0858-2013, Version 2.1, 16 November 2012, NXP
       Secure Smart Card Controllers P5Cx128/P5Cx145 V0v/ V0B(s) Security Target,
       NXP Semiconductors, Business Unit Identification (confidential document)

[7]   Security IC Platform Protection Profile, Version 1.0, 15 June 2007,
       BSI-CC-PP-0035-2007

[8]   Security Target Lite BSI-DSZ-CC-0858-2013, Version 2.1, 16 November 2012, NXP
       Secure Smart Card Controllers P5Cx128V0v/P5Cx145V0v(s) Security Target Lite,
       NXP Semiconductors, Business Unit Identification (sanitised public document)

[9]   Evaluation Technical Report, Version 1.5, 10 May 2013, Evaluation Technical Report
       BSI-DSZ-CC-0858, T-Systems GEI GmbH, (confidential document)

[10]   ETR for composite evaluation according to AIS 36, Version 1.0, 22 April 2013, ETR
       for composition according to AIS36 as summary of the Evaluation Technical Report,
       T-Systems GEI GmbH (confidential document)

[11]   Configuration lists for the TOE:

       •   Configuration List P5Cx128/P5Cx145 V0v/ V0B(s), NXP Semiconductors,
           Business Unit Identification, Rev. 2.0, April 26th, 2013 (confidential document)

---

[8]specifically

•   AIS 25, Version 7, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC
    Supporting Document

•   AIS 26, Version 8,Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL
    Document and CC Supporting Document

•   AIS 31, Version 2, Funktionalitätsklassen und Evaluationsmethodologie für physikalische
    Zufallszahlengeneratoren

•   AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

•   AIS 34, Version 3, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 &
    CCv3.1) and EAL6 (CCv3.1)

•   AIS 35, Version 2.0, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and
    CC Supporting Document and CCRA policies

•   AIS 36, Version 3, Kompositionsevaluierung including JIL Document and CC Supporting Document

•   AIS 38, Version 2.9, Reuse of evaluation results

- Configuration list for composite evaluation P5Cx128/P5Cx145 V0v/ V0B(s), NXP Semiconductors, Business Unit Identification, Rev. 1.9, April 17th, 2013

- Customer-Specific appendix of the Configuration List P5Cx128/P5Cx145 V0v/V0B(s), NXP Semiconductors, Business Unit Identification, Rev. 1.8, April 17th, 2013

- Production flows, P5CD145V0A/B (T051A/B / s051B) P5CN145V0G (T051G) Smart Card Controller, NXP Semiconductors, Business Unit Identification, Rev. 1.28, 13.11.2012

[12]   Guidance documentation for the TOE:

- Guidance, Delivery and Operation Manual, NXP Secure Smart Card Controllers P5Cx128/ P5Cx145, NXP Semiconductors, Version 1.7, Document Number: 185117, 19 March 2013

- Product Data Sheet Addendum Wafer Specification, P5Cx128/P5Cx145 family, NXP Semiconductors, Business Unit Identification, Rev. 3.5, Document Number 184935, 26.04.2013

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

- Data Sheet P5Cx128/P5Cx145 family, Secure dual interface and contact PKI smart card controller, NXP Semiconductors, Rev. 3.5, Document Number 177935, 14 February 2012

This page is intentionally left blank.

C   Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

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

● describes the version of the CC to which the PP or ST claims conformance.

● describes the conformance to CC Part 2 (security functional requirements) as either:

– **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or

– **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.

● describes the conformance to CC Part 3 (security assurance requirements) as either:

– **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or

– CC Part 3 extended - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

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

● Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:

– the SFRs of that PP or ST are identical to the SFRs in the package, or

– the SARs of that PP or ST are identical to the SARs in the package.

● Package name Augmented - A PP or ST is an augmentation of a predefined package if:

– the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.

– the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

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

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

● PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.

● Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D."

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

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

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

APE: Protection Profile evaluation class decomposition"

Class ASE: Security Target evaluation (chapter 11)

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

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

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

"The following Sections describe the constructs used in representing the assurance classes, families, and components."
"Each assurance class contains at least one assurance family."
"Each assurance family contains one or more assurance components."

The following table shows the assurance class decomposition.

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

Assurance Class	Assurance Components
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

"The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility."

Evaluation assurance level (EAL) overview (chapter 8.1)

"Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of "augmentation" allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an "EAL minus a constituent assurance component" is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	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-0858-2013

Evaluation results regarding development and production environment

Common Criteria

The IT product NXP Secure PKI Smart Card Controllers P5CD128V0v/ V0B(s), P5CC128V0v/ V0B(s), P5CD145V0v/ V0B(s), P5CC145V0v/ V0B(s), P5CN145V0v/V0B(s), each including IC Dedicated Software (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by advice of the Certification Body for components beyond EAL 5 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

As a result of the TOE certification, dated 12 June 2013, the following results regarding the development and production environment apply. The Common Criteria assurance requirements ALC – Life cycle support (i.e. ALC_CMC.4, ALC_CMS.5, ALC_DEL.1, ALC_DVS.2, ALC_LCD.1, ALC_TAT.2) are fulfilled for the development and production sites of the TOE listed below:

The target of evaluation (TOE) is developed by:

> NXP Semiconductors Germany GmbH
> Business Unit Identification
> Stresemannallee 101
> D-22529 Hamburg
>
> This site provides also customer support.

The evaluation deliverables are provided by:

> NXP Semiconductors Germany GmbH
> Business Unit Identification
> Stresemannallee 101
> D-22529 Hamburg
>
> or
>
> NXP Semiconductors (Thailand)
> Assembly Plant Bangkok, Thailand (APB)
> 303 Moo 3 Chaengwattana Rd.
> Laksi, Bangkok 10210 Thailand
>
> for the hardware platform and
>
> NXP Semiconductors GmbH
> Business Unit Identification
> Document Control Office
> Mikron-Weg 1
> A-8101 Gratkorn
>
> for the documentation of the TOE.

Following sites are involved for the production of the TOE wafer fab and associated mask shops:

Semiconductor Factory (chipfinishing and wafer production):
Systems on Silicon Manufacturing Co. Pte. Ltd. (SSMC)
70 Pasir Ris Drive 1
Singapore 519527
Singapore

Mask Shop for SSMC:
Toppan Photomasks Korea Ltd.
345-1, Sooha-Ri ShinDoon-Myon
467-840 Ichon
South Korea

Semiconductor Factory (chipfinishing):
GLOBALFOUNDRIES Singapore Pte Ltd.
60 Woodlands Industrial Park D, Street 2
Singapore, 738406

Semiconductor Factory (wafer production):
GLOBALFOUNDRIES Singapore (Tampines) Pte Ltd
1 Tampines Industrial Avenue 5
Singapore 528830

Mask Shop for Globalfoundries:
Photronics Singapore Pte. Ltd.
6 Loyang Industrial Park
Singapore 507099

Mask Shop for Globalfoundries:
Photronics Semiconductors Mask Corp. (PSMC)
1F, No.2, Li-Hsin Rd.
Science-Based Industrial Park
Hsin-Chu City
Taiwan R.O.C.

In addition, the following sites are involved for the bumping, testing, module inlay assembly of the TOE:

Wafer Bumping:
Chipbond Technology Corporation
No. 3, Li-Hsin Rd. V
Science Based Industrial Park
Hsin-Chu City
Taiwan R.O.C.

Test Centre:
NXP Semiconductors GmbH
IC Manufacturing Operations - Test Center Hamburg (IMO TeCH)
Stresemannallee 101
D-22529 Hamburg

Test Centre:
Assembly Plant Kaohsiung
NXP Semiconductors Taiwan Ltd

#10, Jing 5th Road, N.E.P.Z, Kaohsiung 81170
Taiwan, R.O.C

Test Center and Module Assembly:
NXP Semiconductors (Thailand)
Assembly Plant Bangkok, Thailand (APB)
303 Moo 3 Chaengwattana Rd.
Laksi, Bangkok 10210 Thailand

Module Assembly:
NedCard B.V.
Bijsterhuizen 25-29
6604 LM Wijchen
The Netherlands

Module Assembly:
Chipbond Technology Corporation
No. 1, Dàhuá 1st Rd.
Kaohsiung City
Taiwan 806, R.O.C.

Inlay assembly:
HID Global Galway
Paic Tionscail na Tulaigh
Balle na hAbhann
Co. Galway
Ireland

Inlay assembly:
Smartrac Technology Ltd.
142 Moo, Hi-Tech Industrial Estate
Tambon Ban Laean, Amphor Bang-Pa-In
13160 Ayutthaya
Thailand

Inlay assembly:
SMARTRAC TECHNOLOGY GERMANY GmbH
Gewerbeparkstr. 10
51580 Reichshof-Wehnrath
Germany

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.