Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0680-2010

for

NXP Secure Smart Card Controller P5CD080V0B, P5CN080V0B, P5CC080V0B and P5CC073V0B each with specific 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-0680-2010

NXP Secure Smart Card Controller P5CD080V0B, P5CN080V0B, P5CC080V0B and P5CC073V0B each with specific IC Dedicated Software

from	NXP Semiconductors Germany GmbH
PP Conformance:	Smartcard IC Platform Protection Profile, Version 1.0, July 2001, BSI-PP-0002-2001
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_MSU.3 and AVA_VLA.4

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, Version 2.3 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 2.3 (ISO/IEC 15408:2005).

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, 3 November 2010

For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED

Bernd Kowalski L.S.
Head of Department

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A Certification....7

1 Specifications of the Certification Procedure....7
2 Recognition Agreements....7
2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)....8
2.2 International Recognition of CC – Certificates (CCRA)....8
3 Performance of Evaluation and Certification....9
4 Validity of the Certification Result....9
5 Publication....10

B Certification Results....12

1 Executive Summary....13
2 Identification of the TOE....15
3 Security Policy....17
4 Assumptions and Clarification of Scope....17
5 Architectural Information....18
6 Documentation....18
7 IT Product Testing....19
8 Evaluated Configuration....20
9 Results of the Evaluation....20
9.1 CC specific results....20
9.2 Results of cryptographic assessment....21
10 Obligations and Notes for the Usage of the TOE....22
11 Security Target....22
12 Definitions....23
12.1 Acronyms....23
12.2 Glossary....24
13 Bibliography....26

C Excerpts from the Criteria....29

D Annexes....37

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 2.3 (ISO/IEC 15408:2005)[5] [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

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 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

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 smartcard 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.

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 smartcard 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 ACM_SCP.3, ADV_FSP.3, ADV_HLD.3, ADV_IMP.2, ADV_INT.1, ADV_RCR.2, ADV_SPM.3, ALC_DVS.2, ALC_LCD.2, ALC_TAT.2, ATE_DPT.2, AVA_CCA.1, AVA_MSU.3 and AVA_VLA.4 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 Smart Card Controller P5CD080V0B, P5CN080V0B, P5CC080V0B and P5CC073V0B each with specific IC Dedicated Software has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0410-2007. Specific results from the evaluation process BSI-DSZ-CC-0410-2007 were re-used.

The evaluation of the product NXP Secure Smart Card Controller P5CD080V0B, P5CN080V0B, P5CC080V0B and P5CC073V0B each with specific IC Dedicated Software was conducted by T-Systems GEI GmbH. The evaluation was completed on 29 October 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 should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e.

[6] Information Technology Security Evaluation Facility

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 Smart Card Controller P5CD080V0B, P5CN080V0B, P5CC080V0B and P5CC073V0B each with specific 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.

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

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 Smart Card Controller P5CD080V0B, P5CN080V0B, P5CC080V0B and P5CC073V0B each with specific IC Dedicated Software.** The TOE is the hardware of the microcontroller chip P5CD080V0B (short name of the TOE) of the Smart Card Controller IC family produced by NXP. The TOE includes also IC Dedicated Test Software for test purposes and IC Dedicated Support Software, both stored in the Test-ROM of the microcontroller. The Smart Card Controller hardware comprises an 8-bit processing unit, volatile and non-volatile memories accessible via a memory management unit, cryptographic co-processors, security components and three communication interfaces.

The TOE includes a Data Sheet [12], a document describing the Instruction Set [16] and the Guidance Document [11]. This documentation contains a description of the architecture, the secure configuration and usage of the hardware platform by the Smartcard Embedded Software.

The security measures of the P5CD080V0B are designed to act as an integral part of the complete security system in order to strengthen the design as a whole. Several security measures are completely implemented in and controlled by the hardware. Other security measures are controlled by the hardware and allow a configuration by software or software guided exceptions. With the different CPU modes and the memory management unit the TOE is intended to support multi-application projects.

The non-volatile EEPROM can be used as data or program memory. It contains high reliability cells which guarantee data integrity. This is ideal for applications requiring non-volatile data storage and important for the use as memory for native programs. Security Functions protect data in the on-chip ROM, EEPROM and RAM. In particular when being used in the banking and finance market or in electronic commerce applications the smartcard must provide high security.

Hence the TOE shall

- maintain the integrity and the confidentiality of code and data stored in the memories of it and
- maintain the different CPU modes with the related capabilities for configuration and memory access and
- maintain the integrity, the correct operation and the confidentiality of Security Functions (security mechanisms and associated functions) provided by the TOE.

These features are ensured by the construction of the TOE and the Security Functions it provides. The "NXP P5CD080V0B Secure Smart Card Controller" (TOE) mainly provides a hardware platform for a smartcard with

- functions to calculate the Data Encryption Standard (Triple-DES) with up to three keys,
- functions to calculate the Advanced Encryption Standard (AES) with different key lengths,
- support for large integer arithmetic (multiplication, addition and logical) operations, suited for public key cryptography and elliptic curve cryptography,
- a random number generator,
- memory management control features,

- cyclic redundancy check calculation (CRC),
- ISO 7816 contact interface with UART,
- contact-less interface supporting MIFARE and ISO 14443A (configuration P5CD080V0B) or S²C interface (configuration P5CN080V0B).

In addition several security features independently implemented in hardware or controlled by software will be provided to ensure proper operation as well as integrity and confidentiality of stored data. This includes for example measures for memory protection and sensors to allow operation only under specified conditions.

Note: The arithmetic co-processor for large integer arithmetic operations is intended to be used for the calculation of asymmetric cryptographic algorithms. Any asymmetric cryptographic algorithm needs to be implemented in software by using the calculation functions provided by the co-processor. Therefore the co-processor without software does not provide a Security Function itself e.g. cryptographic support. This means that Smartcard Embedded Software that implements e.g. the RSA cryptographic algorithm is not included in the evaluation. Nevertheless the co-processor is part of the Smartcard IC and therefore a security relevant component of the TOE that must resist to the attacks mentioned in the Security Target and that must operate correctly as specified in the Data Sheet. The same scope for the evaluation is applied to the CRC module.

The TOE can be delivered in different configurations. This influences the availability of the contact-less interface (including the functions provided by the MIFARE Operating System) and other not security relevant features. The results of this evaluation are valid for the product configurations called P5CD080V0B, P5CN080V0B, P5CC080V0B and P5CC073V0B. The following table provides an overview about the differences between the P5CD080V0B and the configurations:

TOE	**contact-less interface**	**I/O Pads for ISO 7816**
P5CD080V0B	enabled, configured for ISO 14443A	3
P5CN080V0B	enabled, configured for NFC (S²C)	2
P5CC080V0B	disabled	3
P5CC073V0B	disabled	3

The Security Target [6] is the basis for this certification. It is based on the certified Protection Profile Smartcard IC Platform Protection Profile, Version 1.0, July 2001, BSI-PP-0002-2001 [9].

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_MSU.3 and AVA_VLA.4.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6] and [7], chapter 5.1.1. They are selected from Common Criteria Part 2 and some of them are newly defined in the Protection Profile [9]. Thus the TOE is CC Part 2 extended.

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

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

Table 1: TOE Security Functions

For more details please refer to the Security Target [6] and [7], chapter 6.1.

The claimed TOE's Strength of Functions 'high' (SOF-high) for specific functions as indicated in the Security Target [6] and [7], chapter 6.1 is confirmed. The rating of the Strength of Functions does not include the crypto algorithms suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The assets to be protected by the TOE are defined in the Security Target [6] and [7], 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] and [7], chapter 3.2 to 3.4.

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 Smart Card Controller P5CD080V0B, P5CN080V0B, P5CC080V0B and P5CC073V0B each with specific IC Dedicated Software

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Date	Form of Delivery
1	HW	NXP P5CD080V0B, P5CN080V0B ,P5CC080V0B and P5CC073V0B Secure Smart Card Controller	V0B	GDS 2 File: T035B_20060904.gds2	Wafer, modules and packages (see ST)
2	SW	Test ROM Software *(the IC Dedicated Test Software)*	63	29 November 2006	Included in Test ROM on the chip (tmfos_63.lst)
3	SW	Boot ROM Software (part of the IC	63	29 November	Included in Test ROM on the

No	Type	Identifier	Release	Date	Form of Delivery
		Dedicated Support Software)		2006	chip (tmfos_63.lst)
4	SW	Mifare Operating System (part of the IC Dedicated Support Software)	2.0	24 August 2006	Included in Test ROM on the chip (tmfos_63.lst)
5	DOC	Data Sheet P5Cx012/02x/040/073/080/144V0B family, Secure Dual Interface PKI Smart Card Controller, Objective Data Sheet, NXP Semiconductors, Revision 3.7, Document Number: 126537, 04 June 2010	3.7	04 June 2010	Electronic document [12]
6	DOC	Instruction Set, SmartMX-Family Instruction Set, SmartMX-Family, Secure and PKI Smart Card Controller, Philips Semiconductors, Revision 1.1, Document Number: 084111	1.1	04 July 2006	Electronic document [16]
7	DOC	Guidance, Delivery and Operation Manual for the P5Cx012/02x/040/073/080/144 family, NXP Semiconductors, Version 1.8, Document Number: 129918, 15 February 2010	1.8	15 February 2010	Electronic document [11]

Table 2: Deliverables of the TOE

The hardware part of the TOE is identified by P5CD080V0B, P5CN080V0B ,P5CC080V0B and P5CC073V0B and its specific GDS-file. 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, too. The nameplate T035B is specific for the SSMC (Singapore) production site as outlined in the guidance documentation [11]. This nameplate identifies Version V0B 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 11.7):

- The value 28 hex as Device Coding Byte identifies the chip P5CD080V0B,
- The value 27 hex as Device Coding Byte identifies the chip P5CN080V0B,
- The value 26 hex as Device Coding Byte identifies the chip P5CC080V0B,
- The value 16 hex as Device Coding Byte identifies the chip P5CC073V0B.

Items 2, 3 and 4 in table 2 are not delivered as single pieces, but included in the Test ROM part of the hardware platform. 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.

TOE documentation is delivered either as hardcopy or as softcopy (encrypted) according to defined mailing procedures.

To ensure that the customer receives this evaluated version, the delivery procedures described in [11] have to be followed.

3 Security Policy

The security policy of the TOE is to provide basic Security Functions to be used by the smartcard operating system and the smartcard application thus providing an overall smartcard system security. Therefore, the TOE will implement symmetric cryptographic block cipher algorithms (Triple-DES, 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.

As the TOE is a hardware platform, the security policy of the TOE is also provides protection against leakage of information (e.g. to ensure the confidentiality of cryptographic keys during cryptographic functions performed by the TOE), protection against physical probing, malfunctions, physical manipulations, against access to code and data memory and against 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 smartcard operating system and the application software stored in the User ROM and in the EEPROM are not part of the TOE. The code in the Test ROM of the TOE (IC Dedicated Software) is used by the manufacturer of the smartcard to check the functionality of the hardware platform before TOE Delivery. This was considered as part of the evaluation under the CC assurance aspects ALC for relevant procedures and under ATE for testing.

The TOE is delivered as a hardware unit at the end of the hardware platform manufacturing process (phase 3 of the life cycle defined) or at the end of the IC packaging into modules (phase 4 of the life cycle defined). At these specific points in time the ROM part of the operating system software is already stored in the ROM of the hardware platform and the test mode is completely disabled.

The smartcard applications need the Security Functions of the smartcard operating system based on the security features of the TOE. With respect to security the composition of this TOE, the operating system and the smartcard application is important. Within this composition, the Security Functionality is only partly provided by the TOE and causes dependencies between the TOE Security Functions and the functions provided by the operating system or the smartcard application on top. These dependencies are expressed by environmental and secure usage assumptions as outlined in the user documentation.

Within this evaluation of the TOE, several aspects were specifically considered to support a composite evaluation of the TOE together with an embedded smartcard software (i.e. smartcard operating system and application). This was necessary as NXP Semiconductors Germany GmbH, Business Line Identification is the TOE developer and manufacturer and responsible for specific aspects of handling the embedded smartcard application software in its development and production environment. For those aspects refer to chapter 9 of this report.

The full evaluation results are applicable for chips produced at the IC fabrication SSMC in Singapore indicated by the nameplate (on-chip identifier) T035B.

5 Architectural Information

The NXP P5CD080V0B secure smart card controller is an integrated circuit (IC) providing a hardware platform to a smartcard operating system and Smartcard Embedded Software. A top level block diagram and a list of subsystems can be found within the TOE description of the Security Target [7]. The complete hardware description and the complete instruction set of the NXP P5CD080V0B smartcard controller can be found in the Data Sheet, P5Cx02x/040/073/080/144 family [12] and Instruction Set [16].

For the implementation of the TOE Security Functions basically the components 8-bit CPU, Special Function Registers, Triple-DES Co-Processor, AES co-processor, FameXE Co- Processor, Random Number Generator (RNG), Power Module with Security Sensors and Filters are used. The hardware platform is equipped with a Memory Management Unit and provides different CPU Modes in order to separate different applications running on the TOE. Security measures for Physical Protection are realized within the layout of the whole circuitry.

The Special Function Registers provide the interface to the Security Functions of the TOE when they can be configured or used by the smartcard operating system and the Smartcard Embedded Software. The P5CD080V0B provides different levels of access control to the Special Function Register with the different CPU Modes and additional – configurable – access control to Special Function Registers in the least-privileged CPU Mode, the User Mode.

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 that is not accessible after the start up is finished.

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 Smartcard Embedded Software. Based on the partitioning of the memories the Mifare Operating System is not able to access the Smartcard 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 Smartcard Embedded Software. A limited memory area for the data exchange (between Smartcard Embedded Software and Mifare Operating System) and the access to components of the hardware (by the Mifare Operating System) must be configured by the Smartcard Embedded Software.

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. 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 Functions);
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 hardware platform with respect to different operating conditions and varied process parameters (often also referred to as characterisation tests)
   - special verification tests for the Security Functions 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 Functions and all security mechanisms as identified in the functional specification, and in the high and low level designs.

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 are 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 are 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 (refer to chapter 2 and section 3.2 for details on the TOE configuration) provides the Security Functions as specified by the developer. The test results confirm the correct implementation of the TOE Security Functions.

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

This certification covers the following configurations of the TOE:

- The value 28 hex as Device Coding Byte identifies the chip P5CD080V0B,
- The value 27 hex as Device Coding Byte identifies the chip P5CN080V0B,
- The value 26 hex as Device Coding Byte identifies the chip P5CC080V0B,
- The value 16 hex as Device Coding Byte identifies the chip P5CC073V0B.

For identification of a specific configuration, the Device Coding Bytes stored in the EEPROM can be used (see [12], chapter 11.7). The TOE is identified by the nameplate T035B and specific EEPROM coding as outlined in chapter 2.

All TSF are active and usable. Information on how to use the TOE and its Security Functions by the software is provided within the user documentation.

The different CPU modes are: Boot Mode, Test Mode, Mifare Mode, System Mode and User Mode. For more details please refer to [7, chapter 2.1.1]

As the TOE operates after delivery in System Mode or User Mode and the application software being executed on the TOE can not use the Test Mode, the evaluation was mainly performed in the System Mode and User Mode. For all evaluation activities performed in Test Mode, there was a rationale why the results are valid for the System Mode and User Mode, too.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [8] 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 (AIS 34) and guidance specific for the technology of the product [4].

(i) The Application of CC to Integrated Circuits

(ii) Application of Attack Potential to Smartcards and

(iii) ETR for Composition and

(iv) ETR for Composition: Annex A Composite smartcard evaluation: Recommended best practice

(see [4, AIS 25, AIS 26 and AIS 36]) and [4, AIS 31] (functionality classes and evaluation methodology for physical random number generators) were used. The assurance refinements outlined in the Security Target were followed in the course of the evaluation of the TOE.

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.

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 class ASE
- All components of the EAL 5 package as defined in the CC (see also part C of this report)
- The components ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 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-0410-2007, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on assurance family ALC, ATE and AVA.

The evaluation has confirmed:

- PP Conformance: Smartcard IC Platform Protection Profile, Version 1.0, 11 July 2001, BSI-PP-0002-2001 [9]
- 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_MSU.3 and AVA_VLA.4

The following TOE Security Functions fulfil the claimed Strength of Function:

- F.RNG (random number generator), according to AIS 31 Functionality class P2 High, F.LOG (Logical Protection) contributing to the leakage attacks especially for F.HW_DES (Triple-DES Co-processor) and F.HW_AES (AES Co-processor) by SPA/DPA countermeasures. The scheme interpretations AIS 26 and AIS 31 (see[4]) were used.

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 rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). This holds for: F.HW_DES and F.HW_AES.

The strength of the cryptographic algorithms was not rated in the course of the product certification (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 functions 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 user documentations 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.

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 [10].

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

The guidance documentation [11], [12] and [16], contains all necessary information about the usage of the TOE. NXP will also provide either the Security Target to customers or a “light” version of the Security Target [7], which omits some technical details within the rational but contains the relevant information about the TOE itself. This includes the assumptions about the environment and usage of the TOE and the Security Functions provided by the TOE. Note that this ST is conformant to [4, AIS 35].

Besides the further requirements

- to follow the instructions in the user guidance documents and
- to ensure fulfilment of the assumptions about the environment in the Security Target.

11 Security Target

For the purpose of publishing, the Security Target [7] 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

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

BSIG BSI-Errichtungsgesetz, Act setting up the Federal Office for Information Security

CC Common Criteria for IT Security Evaluation

CPU Central Processing Unit

CRC Cycle redundancy Check Calculation

DEA Data Encryption Algorithm

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

FIPS Federal Information Processing Standard

IC Integrated Circuit

I/O Input/Output

IT Information Technology

ISO International Organization for Standardization

ITSEF Information Technology Security Evaluation Facility

MMU Memory Management Unit

NFC Near Field Communication

PP Protection Profile

RAM Random Access Memory

RNG Random Number Generator

ROM Read Only Memory

SF Security Function

SFP Security Function Policy

SFR Security Functional Requirement

SOF Strength of Function

SPA Simple Power Analysis

ST Security Target

S²C Smart card interface standard, complying with ISO-IEC-18092.

TDEA	Triple Data Encryption Algorithm
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 Asynchronous Receiver and Transmitter
USB	Universal Serial Bus

12.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance 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 entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

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

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

13 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

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

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

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Website

[6] Security Target, Evaluation of the P5CD080V0B, P5CC080V0B, P5CN080V0B and P5CC073V0B Secure Smart Card Controllers, NXP Semiconductors, Business Line Identification, Version 1.9, 14 July 2010 (confidential document)

[7] Security Target Lite, Evaluation of the P5CD080V0B, P5CC080V0B, P5CN080V0B and P5CC073V0B Secure Smart Card Controllers, NXP Semiconductors, Business Line Identification, Version 1.9, 14 July 2010 (sanitized public document)

[8] Evaluation Technical Report BSI-DSZ-CC-0680 NXP P5CD080V0B Secure Smart Card Controller, Version 1.39, 29 October 2010, (confidential document)

[9] Smart Card IC Platform Protection Profile, Version 1.0, July 2001, registered at the German Certification Body under number BSI-PP-0002-2001

[10] ETR for composition, NXP P5CD080V0B Secure 8-bit Smart Card Controller, BSIDSZ-CC-0680, T-Systems GEI GmbH, Version 1.36, 29 October 2010 (confidential document)

[11] Guidance, Delivery and Operation Manual for the P5Cx012/02x/040/073/080/144 family, NXP Semiconductors, Version 1.8, Document Number: 129918, February 15th, 2010 (confidential 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, 7 May 2009, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 1, 25 September 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 5, 17 May 2001, 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

[12] Data Sheet, P5Cx012/02x/040/073/080/144V0B family, Secure Dual Interface PKI Smart Card Controller, Objective Data Sheet, NXP Semiconductors, Revision 3.7, Document Number: 126537, 04 June 2010 (confidential document)

[13] FIPS PUB 46-3 Federal Information Processing Publication Data Standard (DES) Reaffirmed 25 Octtober 1999

[14] Configuration List for composite evaluation of the P5Cx012/02x/040/073/080/144V0B family, NXP Semiconductors, Rev. 1.3, 31 August 2007

[15] Customer specific Appendix of the Configuration List for the composite evaluation of the P5Cx012/02x/040/073/080/144V0B family, NXP Semiconductors, Rev. 1.4, 9 July 2008

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

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

- **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.
- **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

- **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.
- **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

- **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.
- **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

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

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

“The goal of a PP evaluation is to demonstrate that the PP is complete, consistent, technically sound, and hence suitable for use as a statement of requirements for one or more evaluatable TOEs. Such a PP may be eligible for inclusion within a PP registry.

Assurance Class	Assurance Family
Class APE: Protection Profile evaluation	TOE description (APE_DES)
	Security environment (APE_ENV)
	PP introduction (APE_INT)
	Security objectives (APE_OBJ)
	IT security requirements (APE_REQ)
	Explicitly stated IT security requirements (APE_SRE)

Table 3 - Protection Profile families - CC extended requirements”

Security Target criteria overview (Chapter 8.3)

“The goal of an ST evaluation is to demonstrate that the ST is complete, consistent, technically sound, and hence suitable for use as the basis for the corresponding TOE evaluation.

Assurance Class	Assurance Family
Class ASE: Security Target evaluation	TOE description (ASE_DES)
	Security environment (ASE_ENV)
	ST introduction (ASE_INT)
	Security objectives (ASE_OBJ)
	PP claims (ASE_PPC)
	IT security requirements (ASE_REQ)
	Explicitly stated IT security requirements (ASE_SRE)
	TOE summary specification (ASE_TSS)

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

“The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

“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 11.1)

“Table 6 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 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 extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“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 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, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“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 practice. 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 11.5)

“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 practices.

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 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices 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 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices 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 11.8)

“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 11.9)

“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.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.”

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.”

“Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”

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-0680-2010

Evaluation results regarding development and production environment

The IT product NXP Secure Smart Card Controller P5CD080V0B, P5CN080V0B, P5CC080V0B and P5CC073V0B each with specific IC Dedicated Software (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 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 2.3 (ISO/IEC 15408:2005).

As a result of the TOE certification, dated 3 November 2010, the following results regarding the development and production environment apply. The Common Criteria Security Assurance Requirements

- ACM – Configuration management (i.e. ACM_AUT.1, ACM_CAP.4, ACM_SCP.3),
- ADO – Delivery and operation (i.e. ADO_DEL.2, ADO_IGS.1) and
- ALC – Life cycle support (i.e. ALC_DVS.2, ALC_LCD.2, ALC_TAT.2),

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

Site	Address	Function
Hamburg, Hausbruch, Germany	NXP Semiconductors GmbH Business Line Identification Georg-Heyken-Str. 1 D-21147 Hamburg	Development and customer support
Gratkorn, Austria	NXP Semiconductors GmbH Business Line Identification Document Control Office Mikron-Weg 1 A-8101 Gratkorn	Document control
Singapore	Systems on Silicon Manufacturing Co. Pte. Ltd. (SSMC) 70 Pasir Ris Drive 1 Singapore 519527 Singapore	Wafer fab
Singapore	Photronics Singapore Pte. Ltd. 6 Loyang Way 2 Loyang Industrial Park Singapore 507099 Singapore	Mask shop
Hsin-Chu City, Taiwan R.O.C.	Photronics Semiconductors Mask Corp. (PSMC) 1F, No.2, Li-Hsin Rd. Science-Based Industrial Park Hsin-Chu City, Taiwan R.O.C.	Mask shop
Hsin-Chu City, Taiwan R.O.C	Chipbond Technology Corporation, No. 3, Li-Hsin Rd. V, Science Based Industrial Park, Hsin-Chu City, Taiwan	Wafer Bumping

	R.O.C	
Hamburg Lokstedt, Germany	NXP Semiconductors GmbH IC Manufacturing Operations Test Center Hamburg (IMO TeCH) Stresemannallee 101 D-22529 Hamburg	Test Center, assembly, delivery
Bangkok, Thailand	NXP Semiconductors (Thailand) 303 Chaengwattana Rd. Laksi Bangkok 10210 Thailand	Test Center, assembly, delivery
Smartrac Technology GmbH, Germany	Smartrac Technology GmbH Wernerwerkstr. 2 93049 Regensburg Germany	Inlay assembly
Smartrac Technology LTD, Thailand	Smartrac Technology LTD 142 Moo 1 Hi-Tech Industrial Estate, Tambon Ban, Amphor Bang-Pa-in, Phra Nakorn Si Ayutthaya 13160 Thailand	Inlay assembly
HID Global Galway, Irland	HID Global Galway, Paic Tionscail na Tulaigh, Balle na hAbhann, Co. Galway,Ireland	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 [7] are fulfilled by the procedures of these sites.