Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0411-2007

for

NXP Secure Smart Card Controller
P5CD144V0B, P5CN144V0B and P5CC144V0B
each with specific IC Dedicated Software

from

NXP Semiconductors Germany GmbH
Business Line Identification

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

Deutsches IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0411-2007

NXP Secure Smart Card Controller P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software

from

NXP Semiconductors Germany GmbH Business Line Identification

Common Criteria Arrangement for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, version 2.3* (ISO/IEC 15408:2005) extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance for conformance to the *Common Criteria for IT Security Evaluation, version 2.3 (ISO/IEC 15408:2005)*.

Evaluation Results:

PP Conformance:	**Protection Profile BSI-PP-0002-2001**
Functionality:	**BSI-PP-0002-2001 conformant plus product specific extensions** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL 5 augmented by:** ALC_DVS.2 (Life cycle support - Sufficiency of security measures), AVA_MSU.3 (Vulnerability assessment - Analysis and testing for insecure states), AVA_VLA.4 (Vulnerability assessment - Highly resistant)

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.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 5. July 2007

The President of the Federal Office
for Information Security

Dr. Helmbrecht L.S.

IT Security Certified

SOGIS - MRA

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5477, Infoline +49 (0)3018 9582-111

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2)

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.

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 setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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)
- Common Criteria for IT Security Evaluation (CC), version 2.3[5]
- Common Methodology for IT Security Evaluation (CEM), version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

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 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

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective in March 1998. This agreement has been signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7). The German Federal Office for Information Security (BSI) recognizes certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

2.2 International Recognition of CC - Certificates

An arrangement (Common Criteria 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 (CC-MRA). It includes also the recognition of Protection Profiles based on the CC. As of February 2007 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, The Netherlands, New Zealand, Norway, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America.

The current list of signatory nations resp. approved certification schemes can be seen on the web site: http://www.commoncriteriaportal.org

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 products NXP Secure Smart Card P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software have undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0404-2007. For this evaluation specific results from the evaluation process based on BSI-DSZ-CC-0404-2007 were re-used.

The evaluation of the products NXP Secure Smart Card P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software was conducted by T-Systems GEI GmbH, Prüfstelle für IT-Sicherheit. The T-Systems GEI GmbH, Prüfstelle für IT-Sicherheit is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is:

NXP Semiconductors Germany GmbH
Business Line Identification
Stresemannallee 101
D-22502 Hamburg, Germany

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 5. July 2007.

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.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-24 and D1 to D-4.

The product NXP Secure Smart Card P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software has been included in the BSI list of the certified products, which is published regularly (see also Internet: http://www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] NXP Semiconductors Germany GmbH
Business Line Identification
Stresemannallee 101
D-22502 Hamburg, Germany

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.

Contents of the certification results

1 Executive Summary

The TOE is the hardware of the microcontroller chip P5CD144V0B 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, a document describing the Instruction Set and the Guidance Document. This documentation contains a description of the architecture, the secure configuration and usage of the chip by the Smartcard Embedded Software.

The security measures of the P5CD144V0B 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 smart card 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 P5CD144V0B Secure Smart Card Controller" (TOE) mainly provides a hardware platform for a smart card 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 P5CD144V0B) or S²C interface (configuration P5CN144V0B).

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 this 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 also valid for the product variants called P5CC144V0B and P5CN144V0B. The following table provides an overview about the differences between the P5CD144V0B and the variants:

TOE	**contact-less interface**	**I/O Pads for ISO 7816**
P5CD144V0B	enabled, configured for ISO 14443A	3
P5CN144V0B	enabled, configured for NFC (S²C)	2
P5CC144V0B	disabled	3

Table 1: Major configuration options overview

For the detailed description of the differences refer to [7], section 2.2.

The IT products NXP Secure Smart Card P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software were evaluated by T-Systems GEI GmbH, Prüfstelle für IT-Sicherheit. The evaluation was completed on 8. June 2007. The T-Systems GEI GmbH, Prüfstelle für IT-Sicherheit is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor, vendor and distributor is

NXP Semiconductors Germany GmbH
Business Line Identification
Stresemannallee 101
D-22502 Hamburg, Germany

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL 5 augmented (Evaluation Assurance Level augmented). The following table shows the augmented assurance components.

Requirement	**Identifier**
EAL5	TOE evaluation: Semiformally designed and tested
+: ALC_DVS.2	Life cycle support – Sufficiency of security measures
+: AVA_MSU.3	Vulnerability assessment - Analysis and testing for insecure states
+: AVA_VLA.4	Vulnerability assessment - Highly resistant

Table 2: Assurance components and EAL-augmentation

1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 extended as shown in the following tables.

The following SFRs are taken from CC part 2:

Security Functional Requirement	**Identifier**	**Source from PP or added in ST**
FCS	**Cryptographic support**	
FCS_COP.1 [DES]	Cryptographic operation	ST
FCS_COP.1 [AES]	Cryptographic operation	ST
FDP	**User data protection**	

[8] Information Technology Security Evaluation Facility

Security Functional Requirement	**Identifier**	**Source from PP or added in ST**
FDP_ACC.1 [MEM]	Subset access control	ST
FDP_ACC.1 [SFR][9]	Subset access control	ST
FDP_ACF.1 [MEM]	Security Attribute based access control	ST
FDP_ACF.1 [SFR]	Security Attribute based access control	ST
FDP_IFC.1	Subset information flow control	PP
FDP_ITT.1	Basic internal transfer protection	PP
FMT	**Security Management**	
FMT_MSA.1 [MEM]	Management of security attributes	ST
FMT_MSA.1 [SFR]	Management of security attributes	ST
FMT_MSA.3 [MEM]	Static attribute initialisation	ST
FMT_MSA.3 [SFR]	Static attribute initialisation	ST
FMT_SMF.1	Specification of management functions (see also [4, AIS 32, Int065])	ST
FPT	**Protection of the TOE Security Functions**	
FPT_FLS.1	Failure with preservation of secure state	PP
FPT_ITT.1	Basic internal TSF data transfer protection	PP
FPT_PHP.3	Resistance to physical attack	PP
FPT_SEP.1 [PP]	TSF domain separation	PP
FPT_SEP.1 [CONF]	TSF domain separation	ST
FRU	**Resource utilisation**	
FRU_FLT.2	Limited fault tolerance	PP

Table 3: SFRs for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined:

Security Functional Requirement	**Identifier**	Source from PP or added in ST
FAU	**Security audit**	
FAU_SAS.1	Audit storage	PP
FCS	**Cryptographic support**	
FCS_RND.1	Quality metric for random numbers	PP
FMT	**Security management**	
FMT_LIM.1	Limited capabilities	PP

9 [SFR] here means Special Function Register

Security Functional Requirement	Identifier	Source from PP or added in ST
FMT_LIM.2	Limited availability	PP

Table 4: SFRs for the TOE, CC part 2 extended

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST [7], chapter 5.1.1.

The following Security Functional Requirements are defined for the IT-Environment of the TOE:

Security Functional Requirement	Addressed issue
FCS_CKM.1	Cryptographic key generation
FCS_CKM.4	Cryptographic key generation
FDP_ITC.1	Import of user data without security attributes
FMT_MSA.2	Secure security attributes
FMT_SMR.1	Security roles

Table 5: SFRs for the IT-Environment

Note: only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.2.1.

These Security Functional Requirements are implemented by the 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 6: Security Functions

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

1.3 Strength of Function

The TOE's strength of functions is claimed high (SOF-high) for specific functions as indicated in the Security Target [7, chapter 6.1].

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). For details see chapter 9 of this report.

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The threats which were assumed for the evaluation and averted by the TOE and the organisational security policies defined for the TOE are specified in the Security Target and can be summarised as follows.

So called standard high-level security concerns defined in the Protection Profile [9] were derived from considering the end-usage phase (phase 7 of the life cycle as described in the Security Target) as follows:

- manipulation of user data and of the smart card Embedded Software (while being executed/processed and while being stored in the TOE's memories),
- disclosure of user data and of the smart card Embedded Software (while being processed and while being stored in the TOE's memories) and
- deficiency of random numbers.

These high-level security concerns are refined in the Protection Profile [9] and used by the Security Target by defining threats on a more technical level for

- Inherent Information Leakage,
- Physical Probing,
- Physical Manipulation,
- Malfunction due to Environmental Stress,
- Forced Information Leakage,
- Abuse of Functionality and
- Deficiency of Random Numbers.

The development and production environment starting with phase 2 up to TOE delivery are covered by an organisational security policy outlining that the IC developer / manufacturer must apply the policy "Protection during TOE Development and Production (P.Process-TOE)" so that no information is unintentionally made available for the operational phase of the TOE. The Policy ensures confidentiality and integrity of the TOE and its related design information and data. Access to samples, tools and material must be restricted.

Because there is a specific security component which is not derived from threats the developer must apply the policy P.Add-Components (Additional Specific Security Components) for Triple-DES encryption and decryption, AES encryption and decryption, Area based Memory Access Control, Memory separation for different software parts (including IC Dedicated Software and Smart Card Embedded Software), Special Function Register Access Control and Protection of configuration data.

Security objectives are taken from the Protection Profile plus additional ones related to the additional policy (see [7], section 3.4).

1.5 Special configuration requirements

The NXP Secure Smart Card Controller P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software distinguish between five different CPU modes: Boot Mode, Test Mode, Mifare Mode, System Mode and User Mode.

The three modes Boot Mode, Test Mode and Mifare Mode are sub-modes of the so-called Super System Mode. These three modes are not available for the Smartcard Embedded Software developer, they are reserved for the three software components that belong to the TOE (refer to [7], section 2.1). The mapping of modes and software components is one-to-one: In Boot Mode the TOE executes the Boot ROM Software, in Test Mode the TOE executes the Test ROM Software and in Mifare Mode the TOE executes the MIFARE Operating System. Note that the Super System Mode is not a mode on its own: When the TOE is in Super System Mode, it is always either in Boot Mode, Test Mode or Mifare Mode, depending on the settings of an internal register not available for the Smartcard Embedded Software.

There are three major configuration options, denoted by different product names. The products differ in the available interfaces: The P5CD144V0B is equipped with the ISO 7816 interface and the ISO 14443A contact-less interface. The P5CN144V0B differs in the configuration of the contact-less interface for Near Field Communication. The P5CC144V0B does have only the ISO 7816 interface enabled, the contact-less interface is disabled. Details are described in the subsections 2.2 of [7]. Common minor configuration options of all configurations are described in [7], section 2.2.4.

The application software being executed on the TOE can not use the Test Mode. The TOE is delivered as a hardware unit at the end of the chip manufacturing process. At this point in time the operating system software is already stored in the non-volatile memories of the chip and the Test Mode is disabled.

Thus, there are no special procedures for generation or installation that are important for a secure use of the TOE. The further production and delivery processes, like the integration into a smart card, personalisation and the delivery of the smart card to an end user, have to be organised in a way that excludes all possibilities of physical manipulation of the TOE. There are no

special security measures for the start-up of the TOE besides the requirement that the controller has to be used under the well-defined operating conditions and that the requirements on the software have to be applied as described in the user documentation [11] and chapter 10 of this report.

1.6 Assumptions about the operating environment

Since the Security Target claims conformance to the Protection Profile BSI-PP-0002-2001 [9], the assumptions defined in section 3.2 of the Protection Profile are valid for the Security Target of this TOE. With respect to the life cycle defined in the Security Target, phase 1 and the phases from TOE Delivery up to the end of phase 6 are covered by these assumptions from the PP.

The developer of the smart card Embedded Software (phase 1) must ensure:

- the appropriate “Usage of Hardware Platform (A.Plat-Appl)” while developing this software in phase 1. Therefore, it has to be ensured, that the software fulfils the assumptions for a secure use of the TOE. In particular the assumptions imply that developers are trusted to develop software that fulfils the assumptions.
- the appropriate “Treatment of User Data (A.Resp-Appl)” while developing this software in phase 1. The smart card operating system and the smart card application software have to use security relevant user data of the TOE (especially keys and plain text data) in a secure way. It is assumed that the Security Policy as defined for the specific application context of the environment does not contradict the Security Objectives of the TOE. Only appropriate secret keys as input for the cryptographic function of the TOE have to be used to ensure the strength of cryptographic operation.

Protection during packaging, finishing and personalisation (A.Process-Card) is assumed after TOE Delivery up to the end of phase 6, as well as during the delivery to phase 7.

The following additional assumption is assumed in the Security Target:

- Key-dependent functions shall be implemented (if applicable) in the Smart Card Embedded Software in a way that they are not susceptible to leakage attacks (A.Key-Function).
- The Smart Card Embedded Software must provide a function to check initialisation data. The data is defined by the customer and injected by the TOE manufacturer into the non-volatile memory to provide the possibility for TOE identification and for traceability (A.Check-Init).

1.7 Disclaimers

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 P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Date	Form of Delivery
1	HW	NXP Secure Smart Card Controller P5CD144V0B, P5CN144V0B and P5CC144V0B	V0B	GDS 2 File: T034B_20060904.gds2	Sawn Wafer or embedded into specific module package (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 Dedicated Support Software)	63	29 November 2006	Included in Test ROM on the 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, P5Cx02x/040/073/080/144 family, Secure Dual Interface PKI Smart Card Controller	3.1	7 March 2007	Electronic document [12]
6	DOC	Instruction Set, SmartMX-Family	1.1	4 July 2006	Electronic document [15]
7	DOC	Guidance, Delivery and Operation Manual for the P5Cx02x/040/080/144 family	1.5	24 May 2007	Electronic document [11]

Table 7: Deliverables of the TOE

The hardware part of the TOE is identified by NXP Secure Smart Card P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software 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 T034B 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 2B hex as Device Coding Byte identifies the chip P5CD144V0B.
- The value 2A hex as Device Coding Byte identifies the chip P5CN144VOB.
- The value 29 hex as Device Coding Byte identifies the chip P5CC144V0B.

Items 2, 3 and 4 in table 7 are not delivered as single pieces, but included in the Test ROM part of the chip. They are identified by their unique version numbers.

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

To ensure that the customer receives the evaluated version of the chip, either

- the customer picks up the TOE himself at the NXP site NXP Semiconductors Germany GmbH, Business Line Identification, Stresemannallee 101, 22529 Hamburg – Germany (see part D, annex A of this report) as a wafer or specific packages
- the customer picks up the TOE himself at the NXP site, NXP Semiconductors (Thailand), 303 Chaengwattana Rd., Laksi Bangkok 10210, Thailand (see part D, annex A of this report) as a module or in a specific package or
- the TOE is sent by NXP to the customer protected by special ordering, secured transport and tracking measures. Additionally, a FabKey according to the defined FabKey-procedures has to be used to support the secure delivery and the identification of the TOE

as described in [11].

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.

Defined procedures at the development and production sites guarantee that the right versions of the Test ROM Software, Boot ROM Software and Mifare Operating System are implemented into a specific ROM mask for a TOE IC.

3 Security Policy

The security policy of the TOE is to provide basic Security Functions to be used by the Smart Card Operating System and the smart card application thus providing an overall smart card 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 security platform, the security policy of the TOE is also to provide 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 Smart Card 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 smart card to check the functionality of the chips 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 chip 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 chip and the test mode is completely disabled.

The smart card applications need the security functions of the smart card operating system based on the security features of the TOE. With respect to security the composition of this TOE, the operating system and the smart card 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 smart card 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 smart card application software (i.e. smart card 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 smart card 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 from the IC fabrication SSMC in Singapore indicated by the nameplate (on-chip identifier) T034B.

5 Architectural Information

The NXP P5CD144V0B 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 P5CD144V0B smartcard controller can be found in the “Data Sheet, P5Cx02x/040/073/080/144 family”, [12] and “Instruction Set”, [15].

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 CPU 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 P5CD144V0B provides different levels of access control to the SFR 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 following documentation is provided with the product by the developer to the customer for secure usage of the TOE in accordance with the Security Target:

For all, NXP Secure Smart Card Controller P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software

- The Guidance, Delivery and Operation Manual [11],
- Instruction set [15] and
- The Data Sheet [12] for the P5CD144V0B, P5CN144V0B and P5CC144V0B

Additional guidance as outlined in chapter 10 of this report has to be followed.

Note that the customer who buys the TOE is normally the developer of the operating system and/or application software which will use the TOE as hardware computing platform to implement the software (operating system / application software) which will use the TOE.

To support a composite evaluation as defined in AIS 36 [4], the document ETR for Composition [10] is provided for the composite evaluator.

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 chip with respect to different operating conditions and varied process parameters (often also referred to as characterisation tests)
   - special verification tests for 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

The TOE is identified by NXP Secure Smart Card P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software with the nameplate T034B and specific EEPROM coding as outlined above.

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 NXP Secure Smart Card P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software distinguishes between five different CPU modes: Boot Mode, Test Mode, Mifare Mode, System Mode and User Mode.

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

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 identical with EAL 4. For components beyond EAL4 the methodology was defined in co-ordination with the Certification Body [4, AIS 34].

(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.

The verdicts for the CC, Part 3 assurance components (according to EAL 5 augmented and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		**Verdict**
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Partial CM automation	ACM_AUT.1	PASS
Generation support and acceptance procedures	ACM_CAP.4	PASS
Development tools CM coverage	ACM_SCP.3	PASS
Delivery and operation	CC Class ADO	PASS
Detection of modification	ADO_DEL.2	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS

Assurance classes and components		Verdict
Development	CC Class ADV	PASS
Semiformal functional specification	ADV_FSP.3	PASS
Semiformal high-level design	ADV_HLD.3	PASS
Implementation of the TSF	ADV_IMP.2	PASS
Modularity	ADV_INT.1	PASS
Descriptive low-level design	ADV_LLD.1	PASS
Semiformal correspondence demonstration	ADV_RCR.2	PASS
Formal TOE security policy model	ADV_SPM.3	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Sufficiency of security measures	ALC_DVS.2	PASS
Standardised life-cycle model	ALC_LCD.2	PASS
Compliance with implementation standards	ALC_TAT.2	PASS
Tests	CC Class ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: low-level design	ATE_DPT.2	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Covert channel analysis	AVA_CCA.1	PASS
Analysis and testing for insecure states	AVA_MSU.3	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Highly resistant	AVA_VLA.4	PASS

Table 8: Verdicts for the assurance components

The evaluation has shown that:

- the TOE is conform to the Smartcard IC Platform Protection Profile, BSI-PP-0002-2001 [9]
- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL5 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) by SPA/DPA countermeasures. The scheme interpretations AIS 26 and AIS 31 (see [4]) were used.

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2). This holds for the TOE Security Function F.HW_DES (Triple-DES Co-processor) used for Triple-DES encryption and decryption and F.HW_AES (AES Co- processor) used for AES encryption and decryption.

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

The code in the Test ROM of the TOE (IC Dedicated Test Software) is used by the TOE manufacturer to check the chip function 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 results of the evaluation are only applicable for chips from the IC fabrication SSMC in Singapore (see part D, Annex A) indicated by the nameplate (on-chip identifier) T034B and the firmware and software versions as indicated above.

The evaluation results cannot be extended to further versions/derivates of the TOE and/or another production sites without any extra investigations.

The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

To support a composite evaluation of the TOE together with a specific smart card embedded software additional evaluator actions were performed during the TOE evaluation. The results are documented in the ETR for Composition[10] according to [4, AIS 36]. Therefore, the interface between the smart card embedded software developer and the developer of the TOE was examined in detail. The ETR for Composition is intended to be provided to a composite product evaluator.

10 Comments/Recommendations

The guidance documentation [11], [12] and [15], 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.

For evaluations of products or systems including the TOE as a part or using the TOE as a platform (for example smart card operating systems or complete smart cards), the ETR for composition [10] resulting from this evaluation is of importance and shall be given to the succeeding evaluation according to AIS 36. In addition, NXP Semiconductors Germany GmbH is able to provide a customer product related configuration list based on the general configuration list provided for the evaluation [14].

The operational documents [11], [12] and [15] contain necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Annexes

Annex A: Evaluation results regarding the development and production environment (see part D of this report).

12 Security Target

For the purpose of publishing, the Security Target [7] of the Target of Evaluation (TOE) is provided within a separate document. It is a sanitized version of the complete Security Target [6] used for the evaluation performed.

13 Definitions

13.1 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
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

13.2 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.

14 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.

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

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

[6] Security Target, Evaluation of the NXP P5CD144V0B, P5CC144V0B, P5CN144V0B Secure Smart Card Controllers, NXP Semiconductors, Business Line Identification, Version 1.2, March 7th, 2007

[7] Security Target Lite, Evaluation of the NXP P5CD144V0B, P5CC144V0B, P5CN144V0B Secure Smart Card Controllers, NXP Semiconductors, Business Line Identification, Version 1.0, March 21st, 2007 (sanitized public document)

[8] Evaluation Technical Report BSI-DSZ-CC-0411 NXP P5CD144V0B Secure Smart Card Controller version 1.0, Date from June 08th, 2007, (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 P5CD144V0B Secure 8-bit Smart Card Controller, BSI-DSZ-CC-0411, T-Systems GEI GmbH, Version 1.0, 06.06.2007

[11] Guidance, Delivery and Operation Manual for the P5Cx02x/040/080/144 family, NXP Semiconductors, Version 1.5, Document Number: 129915, May 24th, 2007

[12] Data Sheet, P5Cx02x/040/073/080/144 family, Secure Dual Interface PKI Smart Card Controller, Objective Data Sheet, NXP Semiconductors, Revision 3.1, Document Number: 126531, March 7th, 2007

[13] FIPS PUB 46-3 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION DATA ENCRYPTION STANDARD (DES) Reaffirmed 25 Oct. 1999

[14] Configuration List for the NXP P5Cx02x/040/080/144 family of Secure Smart Card Controllers, BSI-DSZ-CC-0404/0410/0411, Version 1.0, NXP Semiconductors, April 10th, 2007

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

[16] FIPS PUB 197 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, ADVANCED ENCRYPTION STANDARD (AES), National Institute of Standards and Technology, 2001 November 26

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:

a) **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.

b) **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:

a) **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.

b) **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:

a) **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.

b) **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:

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

CC Part 3:

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

This page is intentionally left blank.

Annex A of Certification Report BSI-DSZ-0411-2007

Evaluation results regarding development and production environment

The IT product NXP Secure Smart Card P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software (Target of Evaluation, TOE) has been evaluated at an accredited and licensed/ approved evaluation facility using the Common Methodology for IT Security Evaluation, version 2.3 (ISO/IEC 15408:2005), extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance, for conformance to the Common Criteria for IT Security Evaluation, version 2.3 (ISO/IEC15408: 2005).

As a result of the TOE certification, dated 5. July 2007, the following results regarding the development and production environment apply. The Common Criteria 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:

a) NXP Semiconductors Germany GmbH, Business Line Identification (BL ID), Georg-Heyken-Strasse 1, 21147 Hamburg, Germany, (development center)

b) NXP Semiconductors Germany GmbH, IC Manufacturing Operations - Test Center Hamburg (IMO TeCH), Stresemannallee 101, 22529 Hamburg, Germany (assembly, test, delivery)

c) NXP Semiconductors (Thailand), 303 Chaengwattana Rd., Laksi Bangkok 10210, Thailand (assembly, delivery)

d) NXP Semiconductors GmbH, Business Line Identification, Document Control Office, Mikron-Weg 1, 8101 Gratkorn, Austria (delivery)

e) Systems on Silicon Manufacturing Co. Pte. Ltd. 8 (SSMC), 70 Pasir Ris Drive 1, Singapore 519527, Singapore (semiconductor factory)

f) Photronics Singapore Pte. Ltd., 6 Loyang Way 2, Loyang Industrial Park, Singapore 507099, Singapore (mask shop)

g) Photronics Semiconductors Mask Corp. (PSMC), 1F, No.2, Li-Hsin Rd., Science-Based Industrial Park, Hsin-Chu City Taiwan R.O.C. (mask shop)

h) Chipbond Technology Corporation, No. 3, Li-Hsin Rd. V, Science Based Industrial Park, Hsin-Chu City, Taiwan R.O.C. (wafer bumping)

The TOE is manufactured in the IC fabrication SSMC in Singapore indicated by the nameplate (on-chip identifier) T034B.

For all sites listed above, the requirements have been specifically applied for each site and in accordance with the Security Target, Evaluation of the P5CD144V0B, P5CN144V0B and P5CC144V0B Secure Smart Card Controllers, NXP Semiconductors, Business Line Identification, Version 1.2, March 7th, 2007 [6]. The evaluators verified, that the threats are countered and the security objectives for the life cycle phases 2, 3 and 4 up to delivery at the end of phase 3 or 4 as stated in the TOE Security Target are fulfilled by the procedures of these sites.