Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0465-2008

for

NXP Smart Card Controller P5CC037V0A 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-0465-2008

Smart Card Controller

NXP Smart Card Controller P5CC037V0A with specific IC Dedicated Software

from	NXP Semiconductors Germany GmbH
PP Conformance:	Smartcard IC Platform Protection Profile, Version 1.0, July 2001, Eurosmart, 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 Arrangement for components up to EAL 4

Common Criteria

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 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, 20 June 2008

For the Federal Office for Information Security

IT Security Certified

SOGIS - MRA

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, herein after 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) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5]
- Common Methodology for IT Security Evaluation, 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 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 on 3 March 1998.

This agreement was 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) recognises certificates issued by the national certification bodies of France and the United Kingdom within the terms of this Agreement.

---

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

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under 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

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

This evaluation contains the components ALC_DVS.2, AVA_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 Smart Card Controller P5CC037V0A with specific IC Dedicated Software has undergone the certification procedure at BSI.

The evaluation of the product NXP Smart Card Controller P5CC037V0A with specific IC Dedicated Software was conducted by T-Systems GEI GmbH. The evaluation was completed on 7 May 2008. 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.

[6] Information Technology Security Evaluation Facility

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.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods may evolve over time, the resistance of the certified version of the product against new attack methods can be re-assessed if required and the sponsor applies for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme. It is recommended to perform a re-assessment on a regular basis.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5 Publication

The product NXP Smart Card Controller P5CC037V0A 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) 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 Business Line Identification Stresemannallee 101 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.

1 Executive Summary

The Target of evaluation (TOE) is the hardware of the microcontroller chip NXP Smart Card Controller P5CC037V0A with specific IC Dedicated Software 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 coprocessors, security components and one communication interface.

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 NXP Smart Card Controller P5CC037V0A with specific IC Dedicated Software 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 nonvolatile 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 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,
- 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.

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 three modes Boot Mode, Test Mode and Mifare Mode are submodes 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 the beginning of section [9,2.1]). The mapping of modes and software components is one-to-one: In Boot Mode the TOE executes the Boot ROM Software and in Test Mode the TOE executes the Test ROM Software. The Mifare Mode is provided for compatibility purposes within the SmartMX family, the TOE has no associated software for this mode. 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. Available for the developer of the Smartcard Embedded Software are the System Mode and the User Mode. The System Mode provides unlimited access to the hardware components. In the User Mode the access is restricted to the CPU and specific Special Function Registers. For the detailed information about the Hardware refer to section [9, 2.1].

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, Eurosmart, BSI-PP-0002-2001 [10].

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see part C or [3], 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] resp. [9], chapter 5.1. They are selected from Common Criteria Part 2 and additional SFR are defined in the used Protection Profile. Thus the TOE is CC part 2 extended.

The Security Functional Requirements (SFR) relevant for the IT-Environment of the TOE are outlined in the Security Target Lite [9, chapter 5.2].

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.OPC	Control of Operating Conditions

TOE Security Function	Addressed issue
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 Lite [9, chapter 6].

The claimed TOE's strength of functions 'high' (SOF-high) for specific functions as indicated in the Security Target Lite [9, chapter 6] is confirmed. 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.

The assets to be protected by the TOE are defined in the Security Target Lite [9, chapter 3.1]. Based on these assets the security environment is defined in terms of assumptions, threats and policies. This is outlined in the Security Target Lite [9 , chapter 3.1 to 3.4].

This certification covers the following configurations of the TOE:

TOE	FameXE and FameXE RAM	EEPROM [kByte]
P5CC037V0A	enabled	36

Major configuration

For more details refer to chapter 8.

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 Smart Card Controller P5CC037V0A with specific IC Dedicated Software

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of delivery
1	HW	NXP P5CC037V0A Secure Smart Card Controller	V0A (GDS 2 File: T038A_20061208.gds2)	Wafer, modules and package (dice include reference T038A)
2	FW	Test ROM Software (the IC Dedicated Test Software),	Version 73, June 26th, 2007	Stored in theTest ROM on the chip (tmfos_73.hex)

No	Type	Identifier	Release	Form of delivery
3	FW	Boot ROM Software (part of the IC Dedicated Support Software)	Version 73, June 26th, 2007,	included in Test ROM on the chip (tmfos_73.hex)
4	DOC	Data Sheet, P5xC012/02x/037/052 family, Secure Contact PKI Smart Card Controller, Data Sheet, NXP Semiconductors	Revision 3.0, Document Number: 129030, October 22nd, 2007	Electronic document [12]
5	DOC	Instruction Set, SmartMX-Family, Secure and PKI Smart Card Controller, Philips Semiconductors	Document Number:084111, July 04, 2006, Revision 1.1	Electronic document [13]
6	DOC	Guidance, Delivery and Operation Manual for the P5xC012/02x/037/052 family, NXP Semiconductors	Version 1.5, Document Number: 139915, January 23rd, 2008	Electronic document [14]

Table 2: Deliverables of the TOE

The hardware part of the TOE is identified by P5CC037V0A 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 T038A is specific for the SSMC (Singapore) production site as outlined in the guidance documentation [14]. This nameplate identifies Version V0A of the hardware, but does not identify specifically the TOE configurations. For identification of a specific configuration, the Device Coding Bytes stored in the EEPROM can be used (see [12], chapter 11.7):

The value 37 hex as Device Coding Byte identifies the chip P5CC037V0A.

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

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

To ensure that the customer receives the evaluated version of the chip, either the customer picks up the TOE himself at the NXP sites (see Annex D) 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 [14].

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 [14] have to be followed.

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

3 Security Policy

The security policy is expressed by the set of security functional requirements and implemented by the TOE. It covers the following issues:

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 an algorithm to ensure the confidentiality of plain text data by encryption and to support secure authentication protocols and it will provide a random number generator.

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 Triple-DES cryptographic functions performed by the TOE), against physical probing, against malfunctions, against physical manipulations 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 assumptions defined in the Security Target and some aspects of threats and organisational security policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance: Usage of Hardware Platform, Treatment of User Data, Protection during TOE Development and Production, Protection during Packaging, Finishing and Personalisation. Details can be found in the Security Target Lite [9, chapter 4.2].

5 Architectural Information

The NXP Smart Card Controller P5CC037V0A with specific IC Dedicated Software are integrated circuits (IC) providing a platform to a smart card operating system and smart card application software. A top level block diagram and a list of subsystems can be found within the TOE description of the Security Target Lite [9, 2.1]. The complete hardware description and the complete instruction set of the TOE is to be found in the Data Sheet [12] and other guidance documents delivered to the customer, see table 2.

For the implementation of the TOE Security Functions basically the central processing unit (CPU) with memory management unit (MMU), RAM, ROM, EEPROM, security logic, interrupt module, bus system, Random Number Generator (RNG) and the cryptographic operations of the chip are used. Security measures for physical protection are realised within the layout of the whole circuitry. For more details refer to [9, 2.1.1].

The on-chip hardware components are controlled by the Smartcard Embedded Software via Special Function Registers. These registers are correlated to the activities of the CPU, the memory management unit, interrupt control, I/O configuration, EEPROM, timers, UART and the co-processors. The communication with the P5CC037V0A can be performed through an UART or the direct usage of the I/O ports. The Smartcard Embedded Software is stored in the Application-ROM and/or in the EEPROM and is not part of the TOE.

The IC Dedicated Test Software (Test ROM Software) in the Test-ROM of the TOE is used by the TOE Manufacturer of the smartcard to test the functionality of the chip during production only and is completely separated from the use of the embedded software by disabling before TOE delivery. For more details refer to [9, 2.1.2].

The TOE also contains IC Dedicated Support Software which is also stored in the Test-ROM. The IC Dedicated Support Software consists of the Boot ROM Software: This software is executed after each reset of the TOE, i.e. every time when the TOE starts. It sets up the TOE and does some basic configuration [9, 2.1.2].

The TOE includes also functionality to calculate single DES operations, but part of the evaluation is the triple-DES operation only.

6 Documentation

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

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

7 IT Product Testing

The tests performed by the developer were divided into six categories:

1. technology development tests as the earliest tests to check the technology against the specification and to get the technology parameters used in simulations of the circuitry (this testing is not strictly related to Security 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 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 P5CC037V0A with the nameplate T038A 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 P5CC037V0A distinguishes between five different CPU modes: Boot Mode, Test Mode, Mifare Mode, System Mode and User Mode. The Mifare Mode is included for compatibility purposes within the SmartMX family and is disabled.

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

The following guidance specific for the technology was used:

(i) The Application of CC to Integrated Circuits

(ii) The Application of Attack Potential to Smartcards

(iii) Functionality classes and evaluation methodology of physical random number generators

(see [4], AIS 25, AIS 26, AIS 31) were used.

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 augmented 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.
- All components claimed in the Security Target Lite [9, chapter 6] and defined in the CC (see also part C of this report)

The evaluation has confirmed:

- for PP Conformance: Smartcard IC Platform Protection Profile, Version 1.0, July 2001, Eurosmart, BSI-PP-0002-2001 [10]
- for the functionality: PP conformant plus product specific extensions
  Common Criteria Part 2 extended
- for the assurance: Common Criteria Part 3 conformant
  EAL 5 augmented by
  ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4
- The following TOE Security Functions fulfil the claimed Strength of Function: high
  F.RNG – Random Number Generation
  F.LOG – Logical Protection

The cryptographic algorithm of F.HW_DES can also be analysed with permutational or probabilistic methods but that was not part of this evaluations.

In order to assess the strength of function the scheme interpretations AIS 25,26 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 4, Para. 3, Clause 2). This holds for: F.HW_DES.

The TOE is equipped with several hardware accelerators to support the standard cryptographic operations. This security enforcing function is introduced to include the cryptographic operation in the scope of the evaluation as the cryptographic function itself is not used from the TOE security policy. On the other hand these functions are of special interest for the use of the hardware as platform for the software. The component is a hardware DES encryption unit. The key for the cryptographic Triple-DES operations is provided from the Smartcard Embedded Software.

The strength of the cryptographic algorithms was not rated in the course of this evaluation (see BSIG Section 4, Para. 3, Clause 2). The validity period of each algorithm and its bitlength is recommended in the official catalogue [15].

10 Obligations and notes for the usage of the TOE

The operational documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. The TOE is delivered to the Smartcard Embedded Software Developer and the Card Manufacturer. The actual end user obtains the TOE from the Card Manufacturer together with the application which runs on the TOE. The Smartcard Embedded Software Developer receives all necessary recommendations and hints to develop his software in form of the delivered application notes. In addition, the following aspects need to be fulfilled when using the TOE:

The guidance documentation [14] and Data Sheet [12] 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 [9], which omits some technical details within the rationale 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 version of the 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.

When using the arithmetic coprocessor for the implementation of crypto algorithms the following information has to be taken into account:

Periodically a new official catalogue is published on the homepage of the German Federal Network Agency. The current version of the catalogue holds for the strength of the TOE`s cryptographic signature algorithms. The user is obliged to take the information of the current version of [15, published February 5th, 2008, page 376] into account. The periods of the recommended usage of the TOEs algorithms for encryption and decryption listed in 9.2 are

- Signature creation and verification using RSA encryption, decryption and key generation with a keylength from 1024 to 2048 bits. A usage of 2048 bits is recommended. From 1974 bits keylenght the current recommended period of usage is by the end of 2014 [15].
- Signature creation and verification according to ECDSA and Elliptic Curve (EC) key generation standard with 192 - 521 bits key sizes. From 224 bits keylenght the current recommended period of usage is by the end of 2014 [15].

This data is deplaced by a new version of [15].

11 Security Target

For the purpose of publishing, the security target [9] of the target of evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete security target [6] used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12 Definitions

12.1 Acronyms

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

MX Memory eXtension

NFC Near Field Communication

PP Protection Profile

PKC Public Key Cryptography

PSW(H) Program Status Word (High byte)

RAM Random Access Memory

RNG Random Number Generator

ROM Read Only Memory

SAR	Security Assurance Requirement.
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SIM	Subscriber Identity Module
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
TRNG	True Random Number Generator
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 Methology for Information Technology Security Evaluation (CEM), Evaluation Methology, 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 P5CC037V0A Secure Smart Card Controller, NXP Semiconductors, Business Line Identification, Version 1.4, April 16th, 2008 (confidential document)

[7] Evaluation Technical Report, BSI-DSZ-CC-0465, Version 1.1, April 18th, 2008, NXP P5CC037V0A Secure Smart Card Controller, T-Systems (confidential document)

[8] Configuration List for the NXP P5xC012/02x/037/052 family of Secure Smart Card Controllers, BSI-DSZ-CC-0466, Version 1.2, NXP Semiconductors, April 16th, 2008 (confidential document)

[9] Security Target Lite, Evaluation of the P5CC037V0A Secure Smart Card Controller, NXP Semiconductors, Business Line Identification, Version 1.1, April 16th, 2008

[10] Smart card IC Platform Protection Profile, Version 1.0, July 2001, BSI registration ID: BSI-PP-0002-2001, developed by Atmel Smart Card ICs, Hitachi Ltd., Infineon Technologies AG, Philips Semiconductors

[11] ETR for composition for the NXP P5CC037V0A Secure Smart Card Controller, BSIDSZ-CC-0465, T-Systems GEI GmbH, Version 1.1, 16.04.2008 (confidential document)

[8] specifically

- AIS 25, Version 3, 6 August 2007, Anwendung der CC auf Integrierte Schaltungen including JIL Document resp. CC Supporting Document
- AIS 26, Version 3, 6 August 2007, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document resp. CC Supporting Document
- AIS 31, Version 1, 25 Sept. 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 1, 2 July 2001, Übernahme international abgestimmter CC-Interpretationen ins deutsche Zertifizierungsschema.
- AIS 34, Version 1.00, 1 June 2004, Evaluation Methodology for CC Assurance Classes for EAL5+
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document resp. CC Supporting Document and CCRA policies
- AIS 36, Version 2, 12 November 2007, Kompositionsevaluierung including JIL Document resp. CC Supporting Document
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[12] Data Sheet, P5xC012/02x/037/052 family, Secure Contact PKI Smart Card Controller, Data Sheet, NXP Semiconductors, Revision 3.0, Document Number: 129030, October 22nd, 2007

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

[14] Guidance, Delivery and Operation Manual for the P5xC012/02x/037/052 family, NXP Semiconductors, Version 1.5, Document Number: 139915, January 23rd, 2008

[15] Regulierungsbehörde für Telekommunikation und Post: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), German "Bundesanzeiger Nr. 19", published February 5th, 2008, page 376

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 35

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0465-2008

Evaluation results regarding development and production environment

The IT product NXP Smart Card Controller P5CC037V0A 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 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 20 June 2008, 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 (test, delivery)

c) NXP Semiconductors (Thailand), 303 Chaengwattana Rd., Laksi Bangkok 10210, Thailand (test, 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) NXP Semiconductors (Philippines), Assembly Plant Calamba (APC), #9 Mountain Drive Light Industry and Science Park II, Calamba, Laguna, Philippines (package assembly)

i) NedCard B.V., Bijsterhuizen 25-29, 6604 LM Wijchen, The Netherlands (modul assembly)

The TOE is manufactured in the IC fabrication SSMC in Singapore indicated by the nameplate (on-chip identifier) T038A.

For the sites listed above, the requirements have been specifically applied in accordance with the Security Target [9]). 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 [9] are fulfilled by the procedures of these sites.