Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0612-2010

for

Crypto Library V2.2 on P5CC037V0A

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-0612-2010

Crypto Library V2.2 on P5CC037V0A

from	NXP Semiconductors Germany GmbH
PP Conformance:	Smartcard IC Platform Protection Profile, Version 1.0, BSI-PP-0002-2001
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 5 augmented by ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4

Common Criteria Recognition Arrangement for components up to EAL 4

Common Criteria

The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

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

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

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

Bonn, 5 August 2010

For the Federal Office for Information Security

SOGIS IT SECURITY CERTIFIED

Irmela Ruhrmann L.S.
Head of Division

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

This page is intentionally left blank.

Preliminary Remarks

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

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

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

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

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

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

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

Contents

A Certification....7
1 Specifications of the Certification Procedure....7
2 Recognition Agreements....7
2.1 European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)....8
2.2 International Recognition of CC – Certificates (CCRA)....8
3 Performance of Evaluation and Certification....9
4 Validity of the Certification Result....9
5 Publication....10
B Certification Results....11
1 Executive Summary....12
2 Identification of the TOE....13
3 Security Policy....15
4 Assumptions and Clarification of Scope....15
5 Architectural Information....16
6 Documentation....16
7 IT Product Testing....16
7.1 Hardware platform testing....16
7.2 Crypto Library testing....17
8 Evaluated Configuration....17
9 Results of the Evaluation....18
9.1 CC specific results....18
9.2 Results of cryptographic assessment....19
10 Obligations and Notes for the Usage of the TOE....20
11 Security Target....20
12 Definitions....21
12.1 Acronyms....21
12.2 Glossary....22
13 Bibliography....24
C Excerpts from the Criteria....27
D Annexes....35

A Certification

1 Specifications of the Certification Procedure

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

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005)[5] [1]
- Common Methodology for IT Security Evaluation, Version 2.3 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]
- Advice from the Certification Body on methodology for assurance components above EAL4 (AIS 34)

2 Recognition Agreements

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

---

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

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

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

5 Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

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

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

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic).

The new agreement was initially signed by the national bodies of Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom.

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

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

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

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

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

2.2 International Recognition of CC – Certificates (CCRA)

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

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

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

This evaluation contains the components ACM_SCP.3, ADV_FSP.3, ADV_HLD.3, ADV_IMP.2, ADV_INT.1, ADV_RCR.2, ADV_SPM.3, ALC_DVS.2, ALC_LCD.2, ALC_TAT.2, ATE_DPT.2, AVA_CCA.1, AVA_MSU.3, 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 Crypto Library V2.2 on P5CC037V0A has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0550-2008. Specific results from the evaluation process BSI-DSZ-CC-0550-2008 were re-used.

The evaluation of the product Crypto Library V2.2 on P5CC037V0A was conducted by Brightsight BV. The evaluation was completed on 01 June 2010. Brightsight BV is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

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

The product was developed by: NXP Semiconductors Germany GmbH

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

4 Validity of the Certification Result

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

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

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

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

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

---

[6] Information Technology Security Evaluation Facility

5 Publication

The product Crypto Library V2.2 on P5CC037V0A has been included in the BSI list of the certified products, which is published regularly (see also Internet: https://www.bsi.bund.de) and [5]. Further information can be obtained from BSI-Infoline +49 228 9582-111.

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

[7] NXP Semiconductors Germany GmbH
P.O. Box 54 02 40
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 **Crypto Library V2.2 on P5CC037V0A.** The Crypto Library V2.2 and the hardware "NXP SmartMX P5CC037V0A Secure Smart Card Controller" (short SmartMX) combined are providing a platform for security applications.

The “Crypto Library on SmartMX“ is a cryptographic library, which provides a set of cryptographic functions that can be used by the Smartcard Embedded Software. The cryptographic library consists of several binary packages that are intended to be linked to the Smartcard Embedded Software. The Crypto Library on SmartMX provides additional functionality to the developer of Smartcard Embedded Software. It is a supplement of the basic cryptographic features provided by the hardware platform. The Crypto Library on SmartMX implements cryptographic algorithms with countermeasures against the attacks described in this Security Target using the co-processors of the SmartMX to provide a software programming interface for the developer of the Smartcard Embedded Software. A Smartcard Embedded Software developer may create Smartcard Embedded Software to execute on the NXP SmartMX hardware. This software is stored in the User ROM of the NXP SmartMX hardware and is not part of the TOE. For more details refer to the ST [6] and [9], chapter 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, BSI-PP-0002-2001 [10].

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the Security Assurance Requirements of the Evaluation Assurance Level EAL 5 augmented by ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4.

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

The Security Functional Requirements (SFR) relevant for the Environment of the TOE are outlined in the Security Target [6] and [9], chapter 5.2.

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

TOE Security Functions	Addressed issue
F.LOG	Extended Logical Protection
F.DES	DES encryption and decryption
F.RSA_encrypt	RSA encryption
F.RSA_sign	RSA signature generation and verification
F.RSA_public	computation of an RSA public key
F.ECC_GF_p_ECDSA	ECC Signature Generation and Verification
F.ECC_GF_p_DH_KeyExch	Diffie-Hellman Key Exchange
F.SHA	Computation of Secure Hash Algorithms
F.RSA_KeyGen	Generation of RSA key pairs
F.ECC_GF_p_KeyGen	ECC Key Generation

TOE Security Functions	Addressed issue
F.RNG_Access	Software RNG
F.Object_Reuse	Clearing memory areas
F.COPY	Sidechannel resistant copying of memory contents

Table 1: TOE Security Functions

For more details please refer to the Security Target [6] and [9], chapter 6.1.

The claimed TOE's Strength of Functions 'high' (SOF-high) for specific functions as indicated in the Security Target [6] and [9], chapter 6.1.14 is confirmed. The rating of the Strength of Functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2). For details see chapter 9 of this report.

The assets to be protected by the TOE are defined in the Security Target [6] and [9], chapter 3.1. Based on these assets the TOE Security Environment is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6] and [9], chapter 3.2 - 3.4.

This certification covers the Crypto Library V2.2 on the following Hardware: P5CC037V0A. For details refer to chapter 8 (of this report).

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:

Crypto Library V2.2 on P5CC037V0A

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW	NXP P5CC037V0A Secure Smart Card Controller	V0A	Wafer, modules and package (dice include reference T038A)
2	SW	Test ROM Software (the IC Dedicated Test Software)	73, dated 26-06-2007	test ROM on the chip (tmfos_63.lst)
3	SW	Boot ROM Software (part of the IC Dedicated Support Software)	73, dated 26-06-2007	test ROM on the chip (tmfos_63.lst)
4	SW	Crypto Library	2.2, 25-11-2008	binary files
5	DOC	NXP Semiconductors Data Sheet P5xC012/02x/037/052 family; Secure contact PKI smart card controller	Rev. 3.6, 06-04-2009	electronic document
6	DOC	NXP Semiconductors Documentation: Instruction Set SmartMX-Family, Secure Smart Card Controller, Objective Specification	Rev. 1.1, 04-07-2006	electronic document

No	Type	Identifier	Release	Form of Delivery
7	DOC	NXP Semiconductors Guidance, Delivery and Operation Manual for the P5Cx012/02x/037/052 family of Secure Smart Card Controller	Rev. 1.5, 23-01-2010	electronic document
8	DOC	NXP Semiconductors User Guidance: Secured Crypto Library on the P5Cx012/02x/037/052 Family	Rev. 1.6, 06-05-2010	electronic document
9	DOC	NXP Semiconductors User Guidance: Secured Crypto Library on the SmartMX – Pseudo Random Number Generator & Chi-Squared Test Library	Rev. 5.0, 24-08-2007	electronic document
10	DOC	NXP Semiconductors User Guidance: Secured Crypto Library on the SmartMX – Secured DES Library	Rev. 3.0, 24-08-2007	electronic document
11	DOC	NXP Semiconductors User Guidance: Secured Crypto Library on the SmartMX – SHA Library	Rev. 4.1, 12-06-2008	electronic document
12	DOC	NXP Semiconductors User Guidance: Secured Crypto Library on the SmartMX – Secured RSA Library	Rev. 4.4, 30-03-2010	electronic document
13	DOC	NXP Semiconductors User Guidance: Secured Crypto Library on the SmartMX – Secured RSA Key Generation Library	Rev. 4.3, 30-03-2010	electronic document
14	DOC	NXP Semiconductors User Guidance: Secured Crypto Library on the SmartMX – Secured ECC Library	Rev. 1.4, 30-03-2010	electronic document
15	DOC	NXP Semiconductors User Guidance: Secured Crypto Library on the SmartMX – Utility Library	Rev. 1.0, 24-08-2007	electronic document

Table 2: Deliverables of the TOE

The hardware part of the TOE is identified by P5CC037V0A. 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 TSMC (Singapore) production site as outlined in the guidance documentation [24]. 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 [26], chapter 11.7):

The value 37 hex as Device Coding Byte DC2 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 version number of the crypto library can be checked in the guidance documentation as hash values of the constituting files.

The delivery process from NXP to their customers (to phase 4 or phase 5 of the life cycle of the PP) guarantees, that the customer is aware of the exact versions of the different parts of the TOE as outlined above. Further information on secure delivery procedures of the hardware platform are given in [21] and [24].

The Crypto Library is intended to be supplied to “users”, who are developers of operating systems or other software to be embedded into the SmartMX chips. The library will be supplied to the users as a set of binary library files, to enable the “users” to incorporate the crypto library into their operating systems.

It has to be made sure that the user of the Crypto Library receives a correct version of the Crypto Library. The customer has to fill in a so-called Order Entry Form for Crypto Libraries. There he has to ensure to select the correct device and to mark the Common Criteria evaluated check-box to ensure to obtain the library CC certified for this device. More details are given in [12].

The reference of the hardware part of the TOE is checked by visual inspection. The surface of the TOE consists of the label “T038A”. The reference of the software part of the TOE is checked by using the SHA-256 hash values. The values are provided in the user guidance manual [12].

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 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:

Protection during Packaging, Finishing and Personalization, Usage of Hardware Platform, Treatment of User Data, Check of Initialisation Data by the Smartcard Embedded Software, Usage of Key-dependent Functions. Details can be found in the Security Target [6] resp.[9], chapter 4.2 and the Protection Profile BSI-PP-0002-2001.

5 Architectural Information

This chapter provides a high-level description of the IT product and its major components based on the evaluation evidence described in the Common Criteria assurance family entitled “High-level design”. The Smartcard IC Platform Protection Profile [10] describes general requirements for smart card controllers and their support software. The Hardware Security Target Lite [22] defines the functionality of the platform provided by the P5CC037V0A Smart Card Controller (abbreviated SmartMX). The Crypto Library V2.2 on SmartMX is described in [6] and [9]. It provides additional functionality to the developer of Smartcard Embedded Software. It is a supplement of the basic cryptographic features provided by the hardware platform.

The TOE contains a Crypto Library, which provides a set of cryptographic functions that can be used by the Smartcard Embedded Software. The Crypto Library consists of several binary packages that are intended to be linked to the Smartcard Embedded Software. The Smartcard Embedded Software developer links the binary packages that he needs to his Smartcard Embedded Software and the whole is subsequently implemented in the User ROM.

The Crypto Library is implemented as a set of subsystems. The division into subsystems is chosen according to the cryptographic algorithms provided. The Crypto Library subsystems are: DES, RSA, ECC over GF(p), SHA, Random Numbers and Utility.

In addition, the Crypto Library implements a software (pseudo) random number generator which is initialised (seeded) by the hardware random number generator of the SmartMX.

Finally, the TOE includes internal security measures for residual information protection and provides a secure copy routine.

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

7.1 Hardware platform testing

The hardware platform 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 a chip in special hardware;
5. Characterisation and verification tests to release the TOE to production.
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).

Further information on the hardware testing are given in the Certification Report BSI-DSZ-CC-0465-2008 [21].

7.2 Crypto Library testing

For the Crypto Library, the developer has defined an extensive test set. The test set covers all TOE interfaces, and all modes of operation of the implemented algorithms, as well as all available parameters. The evaluator was provided with a copy of the required software and hardware, together with the means required to generate the TOE. This allowed the evaluator to perform the complete test set as defined by the developer, in addition to the tests defined by the evaluator.

The hardware test results are extendable to composite evaluations on this hardware TOE, provided that the TOE is operated according to its guidance and the composite evaluation requirements are met.

The following tests are performed: DES/RNG/SHA functionality, functionality and leakage protection against SPA, DPA and timing attacks and sensitivity to fault injection. All test results were as expected.

All security functions have been tested at least once, by repeating the extensive set of full-automated tests of the developer. Furthermore, the evaluator performed an additional RSA key generation test case.

The testing was largely automated using a test-OS that allows access to the functions. Test scripts were extensively used to verify that the functions return the expected values. Side channel protection and resistance against penetration attacks has been assessed as part of the vulnerability analysis.

The overall conclusion is that the Crypto Library on the SmartMX is protected against attackers possessing a high attack potential for all scenarios considered

8 Evaluated Configuration

This certification covers the following configuration of the TOE:

Crypto Library V2.2 on P5CC037V0A (Singapore, TSMC) Device Coding Byte 37 hex.

The Crypto Library provides DES, Triple-DES (3DES), RSA, RSA key generation, RSA public key computation, ECC over GF(p), ECC over GF(p) key generation, ECC Diffie-Hellman key-exchange, SHA-1, SHA-224 and SHA-256 algorithms.

The TOE supports various key sizes for RSA up to a limit of 5024 bits. Conformance with the evaluation requirement Strength of Function: High requires a minimum key size of 1536 bits. The TOE supports various key sizes for ECC over GF(p) up to a limit of 544 bits. Conformance with the evaluation requirement Strength of Function: High requires a minimum key size of 192 bits.

All the evaluation and certification results are only effective for the correct software and hardware versions of the TOE. Please refer to chapter 2 (Identification of the TOE), where the nameplate T038A (Singapore) and the hash values are stated.

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 EAL 4 extended by advice of the Certification Body for components beyond EAL 4 [4] (AIS 34).

Additionally, the following guidance specific for the technology was used:

(i) Functionality classes and evaluation methodology of deterministic random number generators

(ii) The Application of CC to Integrated Circuits

(iii) Application of Attack Potential to Smart Cards

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

(see [4], AIS 20, AIS 25, AIS 26, AIS 31)

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

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

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the class ASE
- All components of the EAL 5 package as defined in the CC (see also part C of this report)
- The components ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 augmented for this TOE evaluation

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0550-2008, re-use of specific evaluation tasks was possible. Specifically, for ALC the Re-use concept as outlined in AIS 38 was used.

The evaluation has confirmed:

- PP Conformance: Smartcard IC Platform Protection Profile, Version 1.0, 11 July 2001, 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 conform
  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_Access – implementation of a software RNG and tests for the hardware RNG.

  F.LOG – implementation of measures to limit or eliminate the information that might be contained in the shape and amplitude of signals or in the time between events found by measuring such signals. It includes software countermeasures against side channel attacks.

  F.COPY – implementation of a secure copy routine which includes randomization as a countermeasure.

  F.SHA – implements SHA-1, SHA-224 and SHA-256 according to the standard FIPS 180-3. The algorithms SHA-224 and SHA-256 do fulfil the claimed Strength of Function high, the SHA-1 does not. For appropriate usage of the TOE, chapter 10 and [23] should be considered.

In order to assess the Strength of Function the scheme interpretations AIS 20, AIS 25, AIS 26, 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 strength of the cryptographic algorithms was not rated in the course of the product certification (see BSIG Section 4, Para. 3, Clause 2). But Cryptographic Functionalities with a security level of 80 bits or lower can no longer be regarded as secure against attacks with high attack potential without considering the application context. Therefore for these functions it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (www.bsi.bund.de).

The Cryptographic Functionalities: 2-key Triple DES (2TDES), seed for the deterministic random number generator, SHA-1 used as collision-resistent hash function provided by the TOE achieve a security level of maximum 80 Bits (in general contexts).

10 Obligations and Notes for the Usage of the TOE

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

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

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

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

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

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

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

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

The user of the Crypto Library must implement the advices of the hardware user guidance [24]. Important to mention are: Section 5.1: error counter mechanism; Section 6.1: appropriate handling of sensor resets and exceptions. Furthermore, for proper functioning of the countermeasures, the user must ensure that the RNG is properly seeded, as described in [12], section 4.12. Finally, in all circumstances, user guidance must be followed and be carefully considered when certain interfaces are used, in particular [16] and [18].

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 (symmetric crypto-algorithm)
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CBC	Cipher Block Chaining (a block cipher mode of operation)
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DPA	Differential Power Analysis
DRNG	Deterministic Random Number Generator
EAL	Evaluation Assurance Level
ECB	Electronic Code Book (a block cipher mode of operation)
ECC	Elliptic Curve Cryptography (i.e. cryptosystems based on elliptic curves)
EEPROM	Electrically Erasable Programmable ROM
ETR	Evaluation Technical Report
GF(p)	Finite field or Galois field that contains p elements and p is a prime number
IC	Integrated Circuit
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
MMU	Memory Management Unit
MX	Memory eXtension
PKC	Public Key Cryptography
PP	Protection Profile
ROM	Read-Only-Memory
RNG	Random Number Generator
SAR	Security Assurance Requirement
SF	Security Function
SFP	Security Function Policy
SFR	1. as a CC-term: Security Functional Requirement 2. as a technical term of the SmartMX-family: Special Function Register

SHA	Secure Hash Algorithm. SHA-1 returns hash-values with 160 bits length, SHA-224 (sometimes called SHA-2) returns hash-values with 224 bits length and SHA-256 (sometimes called SHA-3) returns hash-values with 256 bits length.
SOF	Strength of Function
SPA	Simple Power Analysis
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TRNG	True Random Number Generator
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy
UART	Universal Asynchronous Receiver and Transmitter

12.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

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

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

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

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

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

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

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

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

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

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

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

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

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

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

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

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

13 Bibliography

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

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

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

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

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

[6] Security Target BSI-DSZ-CC-0612-2010, Version 1.4, 2010-05-10, Crypto Library V2.2 on P5CC037V0A, NXP Semiconductors (confidential document)

[7] Evaluation Technical Report, 1.0, 2010-06-01, ETR Crypto Library V2.2 on P5CC037V0A, Brightsight (confidential document)

[8] Configuration list for the TOE, Version 1.3, 2010-05-11, List of Configuration Items (confidential document)

[9] Security Target Lite BSI-DSZ-CC-0612-2010, Version 1.4, 2010-05-10, Crypto Library V2.2 on P5CC037V0A, NXP Semiconductors (sanitised public document)

[10] Protection Profile BSI-PP-0002.2001, Version 1.0, July 2001, by Atmel Smart Card ICs, Hitachi Europe Ltd., Infineon Technologies AG, Philips Semiconductors

[11] ETR for composite evaluation according to AIS 36 for the Product Crypto Library V2.2 on P5CC037V0A, Version 2.0, 2010-08-03, ETR for composition Crypto Library V2.2

[12] NXP Semiconductors User Guidance: Crypto Library on the P5Cx012/02x/037/052 Family, Revision 1.6, 2010-05-06

---

[8] specifically

- AIS 20, Version 1, 2 December 1999, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 25, Version 6, 7 September 2009, Anwendung der CC auf Integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 26, Version 6, 7 May 2009, Evaluationsmethodologie für in Hardware integrierte Schaltungen including JIL Document and CC Supporting Document
- AIS 31, Version 1, 25 September 2001 Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren
- AIS 32, Version 5, 17 May 2010, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 34, Version 3, 3 September 2009, Evaluation Methodology for CC Assurance Classes for EAL5+ (CCv2.3 & CCv3.1) and EAL6 (CCv3.1)
- AIS 35, Version 2.0, 12 November 2007, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies
- AIS 36, Version 2, 12 November 2007, Kompositionsevaluierung including JIL Document and CC Supporting Document
- AIS 38, Version 2.0, 28 September 2007, Reuse of evaluation results

[13] NXP Semiconductors User Guidance: Secured Crypto Library on the SmartMX – Pseudo Random Number Generator & Chi-Squared Test Library, Revision 5.0, 2007-08-24

[14] NXP Semiconductors User Guidance: Secured Crypto Library on the SmartMX – Secured DES Library, Revision 3.0, 2007-08-24

[15] NXP Semiconductors User Guidance: Secured Crypto Library on the SmartMX – SHA Library, Revision 4.1, 2008-06-12

[16] NXP Semiconductors User Guidance: Secured Crypto Library on the SmartMX – Secured RSA Library, Revision 4.4, 2010-03-30

[17] NXP Semiconductors User Guidance: Secured Crypto Library on the SmartMX – Secured RSA Key Generation Library, Revision 4.3, 2010-03-30

[18] NXP Semiconductors User Guidance: Secured Crypto Library on the SmartMX – Secured ECC Library, Revision 1.4, 2010-03-30

[19] NXP Semiconductors User Guidance: Secured Crypto Library on the SmartMX – Utility Library, Revision 1.0, 2007-08-24

[20] Security Target Lite BSI-DSZ-CC-0465, Secured Crypto Library on the P5CC037V0A, NXP Semiconductors Germany GmbH, Rev. 1.6, 2009-07-16 (sanitised public document)

[21] Certification Report for NXP Secure Smart Card Controller P5CC037V0A with specific IC Dedicated Software, Secured Crypto Library Rel. 2.0, BSI-DSZ-CC-0550-2008, 2008-11-27

[22] Security Target Lite BSI-DSZ-0465, Version 1.6, P5CC037V0A, NXP Semiconductors Germany GmbH, 2009-07-09 (sanitised public document)

[23] Bundesnetzagentur: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), German "Bundesanzeiger Nr. 19", page 426, 2010-02-04

[24] Guidance, Delivery and Operation Manual for the P5Cx012/02x/037/052 Family of Secure Smart Card Controllers, NXP Semiconductors, Business Line Identification, Version 1.5, 2010-01-23

[25] Assurance Continuity Maintenance Report BSI-DSZ-CC-0550-2008-MA-01, NXP Secure Smart Card Controller P5CC037V0A with IC Dedicated Software: Secured Crypto Library Release 2.1, 2008-12-15

[26] Data Sheet P5Cx012/02x/037/052 family, Secure contact PKI smart card controller, NXP Semiconductors Germany GmbH, Rev. 3.6, 2009-04-06

[27] Instruction Set SmartMX-Family, Secure Smart Card Controller, Objective Specification, NXP Semiconductors Germany GmbH, Rev. 1.1, 2006-07-04

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

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

The conformance result consists of one of the following:

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

plus one of the following:

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

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

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

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

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

CC Part 3:

Protection Profile criteria overview (chapter 8.2)

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

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

Table 3 - Protection Profile families - CC extended requirements”

Security Target criteria overview (Chapter 8.3)

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

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

Table 5 - Security Target families - CC extended requirements ”

Assurance categorisation (chapter 7.5)

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

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

Table 1: Assurance family breakdown and mapping”

Evaluation assurance levels (chapter 11)

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

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

Evaluation assurance level (EAL) overview (chapter 11.1)

“Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

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

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

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

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

Table 6: Evaluation assurance level summary”

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

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.”

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

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 11.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 11.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 11.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

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

“Objectives

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

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

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

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

"Application notes

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

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

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Annex B: Evaluation results regarding development and production environment 37

This page is intentionally left blank.

Annex B of Certification Report BSI-DSZ-CC-0612-2010

Evaluation results regarding development and production environment

The IT product Crypto Library V2.2 on P5CC037V0A (Target of Evaluation, TOE) has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation, Version 2.3 extended by advice of the Certification Body for components beyond EAL 4 and guidance specific for the technology of the product for conformance to the Common Criteria for IT Security Evaluation (CC), Version 2.3 (ISO/IEC 15408:2005).

As a result of the TOE certification, dated 5 August 2010, the following results regarding the development and production environment apply. The Common Criteria Security Assurance Requirements

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

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

1. NXP Semiconductors Germany GmbH, Business Line Identification, Georg-Heyken-Str. 1, D-21147 Hamburg, Germany (development center)
2. NXP Semiconductors Germany GmbH, IC Manufacturing Operations - Test Center Hamburg (IMO TeCH), Stresemannallee 101, D-22529 Hamburg, Germany (test, delivery)
3. NXP Semiconductors (Thailand), 303 Chaengwattana Rd., Laksi Bangkok 10210, Thailand (test, assembly, delivery)
4. NXP Semiconductors GmbH, Business Line Identification, Document Control Office, Mikron-Weg 1, 8101 Gratkorn, Austria (delivery)
5. Systems on Silicon Manufacturing Co. Pte. Ltd. (SSMC), 70 Pasir Ris Drive 1, Singapore 519527, Singapore (semiconductor factory)
6. Photronics Singapore Pte. Ltd., 6 Loyang Way 2, Loyang Industrial Park, Singapore 507099, Singapore (mask shop)
7. Photronics Semiconductors Mask Corp. (PSMC), 1F, No.2, Li-Hsin Rd., Science-Based Industrial Park, Hsin-Chu City Taiwan R.O.C. (mask shop)
8. NXP Semiconductors (Philippines), Assembly Plant Calamba (APC), #9 MountainDrive Light Industry and Science Park II, Calamba, Laguna, Philippines (package assembly)
9. NedCard B.V., Bijsterhuizen 25-29, 6604 LM Wijchen, The Netherlands (modul assembly)

The TOE is manufactured in the IC fabrication TSMC 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 [6]). The evaluators verified, that the Threats, Security Objectives and Requirements for the TOE life cycle phases up to delivery (as stated in the Security Target [6] and [9]) are fulfilled by the procedures of these sites.