# Certification Report

| | |
|---|---|
| Sponsor and developer: | ***NXP Semiconductors Germany GmbH,***<br>***Business Unit Identification***<br>**Stresemannallee 101**<br>**D-22529 Hamburg**<br>**Germany** |
| Evaluation facility: | ***Brightsight***<br>**Delftechpark 1**<br>**2628 XJ Delft**<br>**The Netherlands** |
| Report number: | **NSCIB-CC-11-31802-CR** |
| Report version: | **1** |
| Project number: | **NSCIB-CC-11-31802** |
| Authors(s): | **NLNCSA** |
| Date: | **July 5, 2012** |
| Number of pages: | **17** |
| Number of appendices: | **0** |

*Reproduction of this report is authorized provided the report is reproduced in its entirety.*

Head office Apeldoorn:
Boogschutterstraat 11A
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

Location Eindhoven:
De Rondom 1
P.O. Box 6235
5600 HE Eindhoven
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)40 265 0 302

Location Enschede:
Josink Esweg 10
P.O. Box 337
7500 AH Enschede
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 859

TÜV Rheinland Nederland B.V. is a registered company with the Amsterdam Chamber of Commerce under number 27288788
info@nl.tuv.com
www.tuv.com/nl

# Certificate

Standard

Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 3 (ISO/IEC 15408)

Certificate number **PC 4602843**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer

**NXP Semiconductors Germany GmbH, Business Unit Identification**

**Located in Stresemannallee 101, D-22529 Hamburg, Germany**

Product and assurance level

**Crypto Library V2.6 on P5CC008V1A / P5CC012V1A,**

Assurance Package:

- EAL5 augmented with ALC_DVS.2 and AVA_VAN.5

Protection Profile Conformance:

- Security IC Platform Protection Profile, Version 1.0, 15.06.2007; Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0035"

Project number **NSCIB-CC-11-31802-CR**

Evaluation facility

**Brightsight BV located in Delft, the Netherlands**

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 3 (ISO/IEC 18045)

SOGIS IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY MUTUAL RECOGNITION AGREEMENT

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 3.1 Revision 3 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 3. 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 Netherlands scheme for certification in the area of IT security [NSCIB] 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 TÜV Rheinland Nederland B.V. or by other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by TÜV Rheinland Nederland B.V. or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Validity

Date of issue : **06-07-2012**

Certificate expiry : **06-07-2017**

Registration number
Notified Body 0336

PRODUCTS
RvA C 078
Accredited by the Dutch
Council for Accreditation

Managing Director
TÜV Rheinland Nederland B.V.
P.O. Box 541
7300 AM Apeldoorn
The Netherlands

# CONTENTS:

# Foreword

The Netherlands Scheme for Certification in the Area of IT Security (NSCIB) provides a third-party evaluation and certification service for determining the trustworthiness of Information Technology (IT) security products. Under this NSCIB, TÜV Rheinland Nederland B.V. has the task of issuing certificates for IT security products.

A part of the procedure is the technical examination (evaluation) of the product according to the Common Criteria assessment guidelines published by the NSCIB. Evaluations are performed by an IT Security Evaluation Facility (ITSEF) under the oversight of the NSCIB Certification Body, which is operated by TÜV Rheinland Nederland B.V. in cooperation with the Ministry of the Interior and Kingdom Relations.

An ITSEF in the Netherlands is a commercial facility that has been licensed by TÜV Rheinland Nederland B.V. to perform Common Criteria evaluations; a significant requirement for such a license is accreditation to the requirements of ISO Standard 17025, General requirements for the accreditation of calibration and testing laboratories.

By awarding a Common Criteria certificate, TÜV Rheinland Nederland B.V. asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

# Recognition of the certificate

The Common Criteria Recognition Arrangement and SOG-IS logos are printed on the certificate to indicate that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL4. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA) version 3 effective from April 2010 provides mutual recognition of Common Criteria and ITSEC certificates at a basic evaluation level for all products. A higher recognition level for evaluation levels beyond EAL4 (resp. E3-basic) is provided for products in the technical domain of Smart cards and similar Devices. This agreement was initially signed by Finland, France, Germany, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Italy joined the SOGIS-MRA in December 2010. The current list of signatory nations and approved certification schemes can be found on: http://www.sogisportal.eu.

# 1 Executive Summary

This Certification Report states the outcome of the Common Criteria security evaluation of the Crypto Library V2.6 on P5CC008V1A / P5CC012V1A. The developer of the Crypto Library is NXP Semiconductors Germany GmbH, Business Unit Identification located in Hamburg, Germany and they also act as the sponsor of the evaluation and certification. A Certification Report is intended to assist prospective consumers when judging the suitability of the IT security properties of the product for their particular requirements.

The Target of Evaluation – TOE (i.e., the Crypto Library V2.6 on P5CC008V1A / P5CC012V1A) consists of the Crypto Library V2.6 and the NXP SmartMX P5CC008V1A and P5CC012V1A Secure Smart Card Controller. For ease of reading the TOE is often called Crypto Library on SmartMX. The evaluation of the TOE was conducted as a composite evaluation and uses the results of the CC evaluation of the underlying NXP SmartMX P5CC008V1A and P5CC012V1A Secure Smart Card Controller certified under the German CC Scheme on 21 December 2011 (BSI-DSZ-CC-0771-2011 *[HW CERT]*).

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 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 NXP SmartMX smart card processor provides the computing platform and cryptographic support by means of co-processors for the Crypto Library on SmartMX.

The Crypto Library on SmartMX provides DES, Triple-DES (3DES), RSA, RSA key generation, RSA public key computation, SHA-1, SHA-224 and SHA-256 algorithms with countermeasures against the attacks described in the Security Target. The TOE supports various key sizes for RSA up to a limit of 5024 bits. In addition, the Crypto Library implements a software (pseudo) random number generator which is initialized (seeded) by the hardware random number generator of the SmartMX. Finally, the TOE provides a secure copy routine and includes internal security measures for residual information protection. For more details refer to the *[ST]*, chapter 1.4.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on April 17th 2012 with the final delivery of the ETR. The certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*. The certification was completed on July 5th 2012 with the preparation of this Certification Report.

The scope of the evaluation is defined by the Security Target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Crypto Library on SmartMX, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the Crypto Library on SmartMX are advised to verify that their own environment is consistent with the Security Target, and to give due consideration to the comments, observations and recommendations in this certification report.

The results documented in the evaluation technical report *[ETR]*[1] for this product provide sufficient evidence that it meets the EAL5 augmented (EAL5+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ALC_DVS.2 (Sufficiency of security measures) and AVA_VAN.5 (Advanced methodical vulnerability analysis).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3 *[CEM]*, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 3 *[CC]*.

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the Crypto Library V2.6 on P5CC008V1A / P5CC012V1A evaluation meets all the conditions for international recognition of Common Criteria Certificates and that the product will be listed on the NSCIB Certified Products list.

[1] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

It should be noted that the certification results only apply to the specific version of the product as evaluated.

# 2 Certification Results

## 2.1 *Identification of Target of Evaluation*

The Target of Evaluation (TOE) for this evaluation is the Crypto Library V2.6 on P5CC008V1A / P5CC012V1A from NXP Semiconductors Germany GmbH, Business Unit Identification located in Hamburg, Germany.

This report pertains to the TOE which is comprised of the following main components:

| Type | Name | Release | Date | Form of delivery |
|---|---|---|---|---|
| IC Hardware | NXP Secure Smart Card Controllers P5CC008V1A/P5CC012V1A | V1A | T053A_20100917.gds2 | wafer, module, inlay, package (dice have nameplate T053A) |
| IC Dedicated Test Software | Test-Rom Software | 110 | | Test-ROM on the chip acc. to tmfos_110_collected.ms3 |
| IC Dedicated Support Software | Boot-ROM Software | 110 | | Test-ROM on the chip acc. to tmfos_110_collected.ms3 |
| IC Dedicated Support Software | Resource Configuration Software | 110 | | Test-ROM on the chip acc. to tmfos_110_collected.ms3 |
| Software | Crypto Library | 2.6 | 26 March 2010 | Electronic file |

To ensure secure usage a set of guidance documents is provided together with the Crypto Library on SmartMX. Details can be found in section 0 of this report.

The hardware part of the TOE is delivered by NXP either as wafers or in packaged form together with the IC Dedicated Support Software. The Crypto Library is delivered in Phase 1 of the TOE lifecycle (for a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 1.4.5.) as a software package (a set of binary files) to the developers of the Smartcard Embedded Software. The Smartcard Embedded Software may comprise in this case an operating system and/or other smart card software (applications). The Software developers can incorporate the Crypto Library into their product.

As explained in the user guidance, as part of the delivery procedure, the customer shall verify the correctness of the delivered files by calculating the SHA-256 hash value of the delivered files and comparing them to reference values provided in the user guidance. For the identification of the Hardware please refer to section 2.7 of this report.

## 2.2 *Security Policy*

The TOE provides the cryptographic algorithms DES/3DES (ECB, CBC, CBC-MAC), RSA and SHA in addition to the functionality described in the Hardware Security Target *[ST-HW]* for the hardware platform. The cryptographic algorithms (except SHA) are resistant against Side Channel Attacks, including Simple Power Analysis (SPA), Differential Power Analysis (DPA), Differential Fault Analysis (DFA) and timing attacks. Details on the resistance claims are provided in the Security Target *[ST]*.

The TOE provides access to random numbers generated by a software (pseudo) random number generator and functions to perform the required test of the hardware (true) random number generator.

The TOE also includes internal security measures for residual information protection and provides a secure copy routine.

Note that the TOE does not restrict access to the functions provided by the hardware: these functions are still directly accessible to the Smartcard embedded Software.

## 2.3 *Assumptions and Clarification of Scope*

### 2.3.1 Assumptions

The Assumptions defined in the Security Target 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 Packaging, Finishing and Personalization,
- Check of Initialisation Data by the Smartcard Embedded Software,
- Operational Environment for RSA Key Generation function if the insecure mode is selected.

Details can be found in the Security Target *[ST]* chapter 2.

### 2.3.2 Clarification of scope

The evaluation did not reveal any threats to the TOE that are not countered by the evaluated security functions of the product.

## *2.4 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 “TOE design (ADV_TDS)”. The intent of this chapter is to characterise the degree of architectural separation of the major components and to show dependencies between the TOE and products using the TOE in a composition (e.g. dependencies between HW and SW).

The TOE contains a Crypto Library, which provides a set of cryptographic functionalities 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. Please note that the crypto functions are supplied as a library rather than as a monolithic program, and hence a user of the library may include only those functions that are actually required. However, some dependencies exist; details are described in the User Guidance.

The TOE is implemented as a set of subsystems. The division into subsystems is chosen according to the cryptographic algorithms provided. The whole TOE provides DES, Triple-DES (3DES), RSA, RSA key generation, RSA public key computation, SHA-1, SHA-224 and SHA-256 algorithms. In addition, the TOE implements a software (pseudo) random number generator, provides a secure copy routine and includes internal security measures for residual information protection. The library relies on the underlying hardware for some functionality.

## *2.5 Documentation*

The following documentation is provided with the product by the developer to the customer:

| Type | Name | Release | Date | Form of delivery |
|---|---|---|---|---|
| HW Documents | Objective data sheet P5Cx008V1A and P5Cx012V1A family, Secure dual interface and contact PKI smart card controller | | | Electronic document |
| | Objective data sheet addendum P5CC008V1A and P5CC0012V1A Post-Delivery-Configuration Addendum, NXP Semiconductors | | | Electronic document |
| | Instruction Set, SmartMX-Family | 1.1 | 4 July 2006 | Electronic document |
| | P5CC008V1A and P5CC012V1A, Guidance, Delivery and Operation<br>Manual | | | Electronic document |
| SW Documents | Secured Crypto Library on the P5CC008V1A and P5CC012V1A family | Rev 1.1 | 25 June 2012 | Electronic document |
| | Secured Crypto Library on the SmartMX – Pseudo Random Number Generator & Chi-Squared Test Library | Rev 5.0 | 24 August 2007 | Electronic document |
| | Secured Crypto Library on the SmartMX – Secured DES Library | Rev 3.0 | 24 August 2007 | Electronic document |

| Type | Name | Release | Date | Form of delivery |
|---|---|---|---|---|
| | Secured Crypto Library on the SmartMX – SHA Library | Rev 4.1 | 12 June 2008 | Electronic document |
| | Secured Crypto Library on the SmartMX – Secured RSA Library | Rev 4.5 | 15 April 2010 | Electronic document |
| | Secured Crypto Library on the SmartMX – Secured RSA Key Generation Library | Rev 4.3 | 30 March 2010 | Electronic document |
| | Secured Crypto Library on the SmartMX – Utility Library | Rev 1.0 | 24 August 2007 | Electronic document |

## *2.6 IT Product Testing*

Testing (depth, coverage, functional tests, independent testing): The evaluators examined the developer’s testing activities documentation and verified that the developer has met their testing responsibilities.

### 2.6.1 Testing approach and depth

For the Crypto Library, the developer has performed extensive testing on FSP, subsystem and module level. All parameter choices have been addressed at least once; all cryptographic operations with keys of all sizes have been tested at least once. All boundary cases identified have been tested explicitly, and additionally the near-boundary conditions have been covered probabilistically. The testing was largely automated using a test-OS that allows access to the functionalities. Test scripts were extensively used to verify that the functions return the expected values.

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 developer has provided the evaluators with their test program and the full set of test scripts (i.e. the “test vectors”), and samples to perform the complete test set as defined by the developer, in addition to the tests defined by the evaluator.

The independent testing comprised of the evaluator repeating a small subset of the developer systems tests on the TOE in the context of ATE_IND.2-4. The rationale for this small subset was based on the fact that the evaluators already performed the full set of developer test on an identical crypto library evaluated under the German scheme and that only spot checking was necessary.

In addition the evaluator performed independent testing in the context of ATE_IND.2-6. The evaluator has selected the following items to be tested:

- Ø Correctness of operation during RSA key generation;
- Ø Side channel protection mechanisms;
- Ø Verification of the developer's PRNG test results.

### 2.6.2 Independent Penetration Testing

The evaluator independent penetration tests were conducted according to the following testing approach:

1. During evaluation of the ADV, ATE and ALC classes the evaluators hypothesized possible vulnerabilities. This resulted in a shortlist of possible vulnerabilities to be further analysed in AVA using the design knowledge gained in particular from the source code analysis in IMP and from the hardware ‘ETR for composition’. This resulted in a shortlist of potential vulnerabilities to be tested.
2. Next the evaluators analysed the TOE design and implementation for resistance against the *[JIL]* attacks. This resulted in further potential vulnerabilities to be tested.
3. The evaluators made an analysis of the TOE in its intended environment to check whether the developer vulnerability analysis in ARC has assessed all information.

4. The evaluators concluded that a number of areas could be potentially vulnerable for attackers possessing a high attack potential. Consequently practical penetration testing was performed for absolute assurance.

### 2.6.3 Test Configuration

Since the TOE is not an end-user product it is not possible to perform testing without first embedding it in a testable configuration. To this end, the developer has created a proprietary test operating system. The main purpose of the test OS is to provide access to the crypto library's functionality. The test OS, and its documentation, as defined in the table below, was provided to the evaluators, and was used in all the testing.

The following items were used to provide support during the tests:

- A set of card samples (the TOE) containing
  - Hardware sample (P5CC012V1A);
  - Cryptographic library version 2.6;
  - TestOS.
- A toolset provided by the developer in order to facilitate re-creation of the Cryptographic library, and loading the library and the TestOS into samples.

### 2.6.4 Testing Results

The testing activities, including configurations, procedures, test cases, expected results and observed results are summarised in the *[ETR]*, with references to the documents containing the full details.

The developer's tests and the independent functional tests produced the expected results, giving assurance that the TOE behaves as specified in its ST and functional specification.

No exploitable vulnerabilities were found with the independent penetration tests.

## *2.7 Evaluated Configuration*

The TOE is defined uniquely by its name and version number Crypto Library V2.6 on P5CC008V1A / P5CC012V1A. The TOE consists of a hardware part and a software part. This certification covers the following configurations of the TOE:

Crypto Library V2.6 on P5CC008V1A with device coding bytes as follows:

| device | DC(0) | DC(1) | DC(2) |
|---|---|---|---|
| P5CC008 | 0x11 | 0x01 | 0x60 |
| P5CC008 | 0x11 | 0x05 | 0x60 |
| P5CC008 | 0x11 | 0x81 | 0x60 |
| P5CC008 | 0x11 | 0x85 | 0x60 |

Crypto Library V2.6 on P5CC012V1A with device coding bytes as follows:

| device | DC(0) | DC(1) | DC(2) |
|---|---|---|---|
| P5CC012 | 0x11 | 0x01 | 0x61 |
| P5CC012 | 0x11 | 0x05 | 0x61 |
| P5CC012 | 0x11 | 0x81 | 0x61 |
| P5CC012 | 0x11 | 0x85 | 0x61 |

The hardware part of the TOE is identified by P5CC008V1A / P5CC012V1A and can be checked by visual inspection and reading out the appropriate memory locations in memory. A so-called nameplate (on-chip identifier) is coded in a metal mask onto the chip during production and can be visually inspected by the customer. The nameplate “T053A” is specific for the SSMC (Singapore) production site. The identification in memory consists of the device coding bytes as mention in the tables above.

The reference of the software part of the TOE is checked by calculating the SHA-256 hash value of the delivered files and comparing them to reference values provided in the user guidance.

## 2.8 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[2] which references several Intermediate Reports and other evaluator documents. To support composite evaluations according to *[CCDB-2007-09-01]* a derived document *[ETRfC]* was provided and approved. This document provides details of the TOE evaluation that have to be considered when this TOE is used as platform in a composite evaluation.

The verdict of each claimed assurance requirement is given in the following tables:

| **Development** | | **Pass** |
|---|---|---|
| Security architecture | ADV_ARC.1 | Pass |
| Functional specification | ADV_FSP.5 | Pass |
| Implementation representation | ADV_IMP.1 | Pass |
| TSF internals | ADV_INT.2 | Pass |
| TOE design | ADV_TDS.4 | Pass |

| **Guidance documents** | | **Pass** |
|---|---|---|
| Operational user guidance | AGD_OPE.1 | Pass |
| Preparative procedures | AGD_PRE.1 | Pass |

| **Life-cycle support** | | **Pass** |
|---|---|---|
| Configuration Management capabilities | ALC_CMC.4 | Pass |
| Configuration Management scope | ALC_CMS.5 | Pass |
| Delivery | ALC_DEL.1 | Pass |
| Development security | ALC_DVS.2 | Pass |
| Life-cycle definition | ALC_LCD.1 | Pass |
| Tools and techniques | ALC_TAT.2 | Pass |

| **Security Target** | | **Pass** |
|---|---|---|
| Conformance claims | ASE_CCL.1 | Pass |
| Extended components definition | ASE_ECD.1 | Pass |
| ST introduction | ASE_INT.1 | Pass |
| Security objectives | ASE_OBJ.2 | Pass |
| Security requirements | ASE_REQ.2 | Pass |
| Security problem definition | ASE_SPD.1 | Pass |
| TOE summary specification | ASE_TSS.1 | Pass |

| **Tests** | | **Pass** |
|---|---|---|
| Coverage | ATE_COV.2 | Pass |

[2] The Evaluation Technical Report contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

| | | |
|---|---|---|
| Depth | ATE_DPT.3 | Pass |
| Functional tests | ATE_FUN.1 | Pass |
| Independent testing | ATE_IND.2 | Pass |

| **Vulnerability assessment** | | **Pass** |
|---|---|---|
| Vulnerability analysis | AVA_VAN.5 | Pass |

Based on the above evaluation results the evaluation lab concluded the Crypto Library V2.6 on P5CC008V1A / P5CC012V1A to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 5 augmented by ALC_DVS.2 and AVA_VAN.5**. This implies that the product satisfies the security technical requirements specified in Security Target Crypto Library V2.6 on P5CC008V1A and P5CC012V1A, Rev. 1.1 – 4 July 2012.

The Security Target claims ‘strict conformance’ to the Security IC Platform Protection Profile, Version 1.0, 15.06.2007; Registered and Certified by Bundesamt für Sicherheit in der Informationstechnik (BSI) under the reference *[BSI-PP-0035]*.

## 2.9 Comments/Recommendations

The operational documents as outlined in section 2.5 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 strength of the implemented cryptographic algorithms was not rated in the course of this evaluation. To fend off attackers with high attack potential appropriate cryptographic algorithms with adequate key lengths must be used (references can be found in national and international documents and standards).

The user of the Crypto Library must implement the advices of the user guidance of both the software and hardware part of the TOE. In particular those advices related to countermeasures against attacks.

Furthermore, for proper functioning of the countermeasures, the user must ensure that the RNG is properly seeded.

Finally, in all circumstances, user guidance must be followed and be carefully considered when certain interfaces are used.

# 3 Security Target

The Security Target Crypto Library V2.6 on P5CC008V1A and P5CC012V1A, Rev. 1.1 – 4 July 2012 is included here by reference. Please note that for the need of publication a public version (Security Target Lite Crypto Library V2.6 on P5CC008V1A and P5CC012V1A, Rev. 1.1 – 4 July 2012) has been created and verified according to *[ST-SAN]*.

# 4 Definitions

This list of Acronyms and the glossary of terms contains elements that are not already defined by the CC or CEM:

| | |
|---|---|
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| CBC | Cipher Block Chaining (a block cipher mode of operation) |
| CBC-MAC | Cipher Block Chaining Message Authentication Code |
| DES | Data Encryption Standard |
| DFA | Differential Fault Analysis |
| ECB | Electronic Code Book (a block cipher mode of operation) |
| IC | Integrated Circuit |
| IT | Information Technology |
| ITSEF | IT Security Evaluation Facility |
| NSCIB | Nederlands Schema voor Certificatie op het gebied van IT-Beveiliging |
| PP | Protection Profile |
| PRNG | Pseudo Random Number Generator |
| RMI | Remote Method Invocation |
| RSA | Rivest-Shamir-Adleman Algorithm |
| SHA | Secure Hash Algorithm |
| SPA/DPA | Simple/Differential Power Analysis |
| TOE | Target of Evaluation |

# 5 Bibliography

This section lists all referenced documentation used as source material in the compilation of this report:

[BSI-PP-0035] "Security IC Platform Protection Profile", Version 1.0, June 2007.

[CC] Common Criteria for Information Technology Security Evaluation, Parts I version 3.1 revision 1, and Part II and III, version 3.1 revision 3.

[CCDB-2007-09-01] CCDB Supporting Document, Composite product evaluation for Smartcards and similar devices, v1.0, Revision 1, September 2007.

[CEM] Common Methodology for Information Technology Security Evaluation, version 3.1, Revision 3, July 2009.

[ETR] Brightsight, Evaluation Technical Report, Crypto Library V2.6 on P5CC008V1A / P5CC012V1A – EAL5+, Version 5.0, July 5, 2012.

[ETRfC] Brightsight, Evaluation Technical Report for Composition, Crypto Library V2.6 on P5CC008V1A / P5CC012V1A – EAL5+, Version 4.0, July 5, 2012.

[ETR-HW] Evaluation Technical Report for composition P5CC012V1A and derivative P5CC008V1A chip for NXP according to AIS36, Version 1.0, November 21, 2011.

[HW-CERT] Certification Report BSI-DSZ-CC-0771-2011, 21 December 2011, NXP Secure Smart card Controllers P5CC008V1A, P5CC012V1A each including ID Dedicated Software.

[JIL] Attack methods for Smart cards and similar devices, JIL, version 2.0, February 2011.

[NSCIB] Nederlands Schema for Certification in the Area of IT Security, Version 1.2, 9 December 2004.

[ST] NXP, Crypto Library V2.6 on P5CC008V1A and P5CC012V1A, Rev. 1.1 – 4 July 2012.

[ST-HW] NXP Secure Smart Card Controllers P5CC008V1A, P5CC012V1A each including IC Dedicated Software Security Target, NXP Semiconductors, Business Unit Identification, Rev. 1.0, 24. May 2011, BSI-DSZ-CC-0771

[ST-SAN] ST sanitising for publication, CC Supporting Document CCDB-2006-04-004, April 2006.

(This is the end of this report).