Certification Report

Crypto Library V1.0 on P60x080/052/040PVC

Sponsor and developer: ***NXP Semiconductors Germany GmbH,***
Business Unit Identification
Stresemannallee 101
D-22529 Hamburg
Germany

Evaluation facility: ***Brightsight***
Delftechpark 1
2628 XJ Delft
The Netherlands

Report number: **NSCIB-CC-12-36243-CR**

Report version: **1**

Project number: **NSCIB-CC-12-36243**

Authors(s): **Wouter Slegers**

Date: **July 29th, 2013**

Number of pages: **17**

Number of appendices: **0**

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 Apeldoorn:
Vissenstraat 6
P.O. Box 541
7300 AM Apeldoorn
The Netherlands
Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

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	**C12-36243**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer	**NXP Semiconductors Germany GmbH, Business Unit Identification** **Stresemannallee 101, D-22529 Hamburg, Germany**
Product and assurance level	**Crypto Library V1.0 on P60x080/052/040PVC,** Assurance Package: ▪ EAL6 augmented with ASE_TSS.2 and ALC_FLR.1 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-12-36243-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)

Common Criteria Recognition Arrangement for components up to EAL4

The IT product identified in this certificate has been evaluated at an accredited and licensed/approved evaluation facility using the Common Methodology for IT Security Evaluation version 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 : **02-08-2013**

Certificate expiry : **02-08-2018**

Registration number

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

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

www.tuv.com/nl

TÜVRheinland®
Precisely Right.

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.

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 related to specific technical domains. 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, approved certification schemes and the list of technical domains for which the higher recognition applies 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 V1.0 on P60x080/052/040PVC. 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.

This Certification Report is a "delta" with respect to the evaluation of the "Crypto Library V1.0 on P60D024/016/012PVB" (NSCIB-CC-12-36242). The changes are solely related to another variant of the underlying Secure Smart Card Controller.

The Target of Evaluation – TOE (i.e., the Crypto Library V1.0 on P60x080/052/040PVC) consists of the Crypto Library V1.0 and the NXP SmartMX2 P60x080/052/040PVC Secure Smart Card Controller. For ease of reading the TOE is often called Crypto Library on SmartMX2. The evaluation of the TOE was conducted as a composite evaluation and uses the results of the CC evaluation of the underlying NXP SmartMX2 P60x080/052/040PVC Secure Smart Card Controller certified under the German CC Scheme on June 24, 2013 (BSI-DSZ-CC-0837 *[HW CERT]*).

The Crypto Library on SmartMX2 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 arbitrary memory of the hardware platform. The NXP SmartMX2 smart card processor provides the computing platform and cryptographic support by means of co-processors for the Crypto Library on SmartMX2.

The Crypto Library on SmartMX2 provides AES, DES, Triple-DES (3DES), RSA, RSA key generation, RSA public key computation, ECDSA, ECC key generation, ECDH, ECC point addition, ECC curve parameter verification, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 algorithms. In addition, the Crypto Library implements a software (pseudo) random number generator, which is initialised (seeded) by the hardware random number generator of the SmartMX2. Finally, the TOE provides a secure copy routine and a secure compare routine and includes internal security measures for residual information protection. For more details refer to the *[ST]*, chapter 1.3.2.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands and was completed on July 24th, 2013 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 29th, 2013 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 SmartMX2, 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 SmartMX2 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 EAL6 augmented (EAL6+) assurance requirements for the evaluated security functionality. This assurance level is augmented with ASE_TSS.2 (TOE summary specification with architectural design summary) and ALC_FLR.1 (Basic flaw remediation).

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]*.

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

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the Crypto Library V1.0 on P60x080/052/040PVC 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. 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 V1.0 on P60x080/052/040PVC 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 Controller P60x080/052/040PVC	VC	10 April 2012	wafer, module, inlay, package (dice have nameplate 9049A)
IC Dedicated Test Software	Test-ROM Software	0A.05	07 May 2012	Test-ROM on the chip acc. to 9049A_LA001_TESTROM_v1 _btos_0Av05_fos_6v10.hex
Security IC Dedicated Support Software	Boot-ROM Software	0A.05	07 May 2012	Boot-ROM on the chip acc. to 9049A_LA001_TESTROM_v1 _btos_0Av05_fos_6v10.hex
	Firmware Operating System (FOS)	6.11	07 May 2012	Firmware Operating System on the chip acc. to 9049A_LA001_TESTROM_v1 _btos_0Av05_fos_6v10.hex
Library file	phSmx2ClAes.lib	1.0	2012-12-05	Electronic file
	phSmx2ClDes.lib	1.0	2012-12-05	Electronic file
	phSmx2ClRsa.lib	1.0	2012-12-05	Electronic file
	phSmx2ClRsaKg.lib	1.0	2012-12-05	Electronic file
	phSmx2ClEccGfp.lib	1.0	2012-12-05	Electronic file
	phSmx2ClSha.lib	1.0	2012-12-05	Electronic file
	phSmx2ClSha512.lib	1.0	2012-12-05	Electronic file
	phSmx2ClRng.lib	1.0	2012-12-05	Electronic file
	phSmx2ClUtils.lib	1.0	2012-12-05	Electronic file
Header file	phSmx2ClAes.h	1.0	2012-12-05	Electronic file
	phSmx2ClDes.h	1.0	2012-12-05	Electronic file
	phSmx2ClRsa.h	1.0	2012-12-05	Electronic file
	phSmx2ClRsaKg.h	1.0	2012-12-05	Electronic file
	phSmx2ClEccGfp.h	1.0	2012-12-05	Electronic file
	phSmx2ClSha.h	1.0	2012-12-05	Electronic file
	phSmx2ClSha512.h	1.0	2012-12-05	Electronic file
	phSmx2ClRng.h	1.0	2012-12-05	Electronic file
	phSmx2ClUtils.h	1.0	2012-12-05	Electronic file
	phSmx2ClUtils_ImportExportFcts.h	1.0	2012-12-05	Electronic file
	phSmx2ClUtils_RngAccess.h	1.0	2012-12-05	Electronic file
	phSmx2ClTypes.h	1.0	2012-12-05	Electronic file
Source code	phSmx2ClUtils_ ImportExportFcts.a51	1.0	2012-12-05	Electronic file
	phSmx2ClUtils_ RngAccess.a51	1.0	2012-12-05	Electronic file

To ensure secure usage a set of guidance documents is provided together with the Crypto Library on SmartMX2. Details can be found in section 2.5 of this report.

The hardware part of the TOE is delivered by NXP either as wafer, module or HVQFN32 SMD 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 1.3.5.) 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 2.8 of this report.

2.2 Security Policy

The TOE provides the cryptographic algorithms AES, DES, Triple-DES (3DES), RSA, RSA key generation, RSA public key computation, ECDSA, ECC key generation, ECDH, ECC point addition, ECC curve parameter verification, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 algorithms 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. SHA is only resistant against Side Channel Attacks and timing attacks. Details on the resistance claims are provided in the Security Target *[ST],* relevant details are provided in the user guidance documents.

The TOE implements a software (pseudo) random number generator, which is initialised (seeded) by the hardware random number generator of the SmartMX2.

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

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,

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 arbitrary memory of the hardware platform. 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 AES, DES, Triple-DES (3DES), RSA, RSA key generation, RSA public key computation, ECDSA, ECC key generation, ECDH, ECC point addition, ECC curve parameter verification, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512 algorithms in addition to the functionality described in the Hardware Security Target *[ST-HW]* for the hardware platform. In addition, the TOE implements a software (pseudo) random number generator, which is initialised (seeded) by the hardware random number generator of the SmartMX2.

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

2.5 Documentation

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

Name	Release	Date	Form of delivery
Product Data Sheet SmartMX2 family P60x040/052/080 VC, Secure high-performance smart card controller	3.0	31 October 2012	Electronic document
Instruction Set for the SmartMX2 family, Secure high-performance smart card controller	3.1	2 February 2012	Electronic document
NXP Secure Smart Card Controller P60x040/052/080VC Guidance and Operation Manual	1.0	22 November 2012	Electronic document
SmartMX2 family P60x040/052/080 VC Wafer and delivery specification	3.1	08 February 2013	Electronic document
Product data sheet addendum: SmartMX2 family, Post Delivery Configuration (PDC)	3.1	12 December 2012	Electronic document
Product data sheet addendum: SmartMX2 family, Chip Health Mode (CHM)	3.0	11 May 2012	Electronic document
Product data sheet addendum: SmartMX2 family, Firmware Interface Specification (FIS)	3.3	11 December 2012	Electronic document
SmartMX2 Crypto Library: User Guidance – Crypto Library on SmartMX2	1.0	2012-12-05	Electronic document
SmartMX2 Crypto Library: User Manual – Random Number Generator	1.0	2012-12-05	Electronic document
SmartMX2 Crypto Library: User Manual – AES	1.0	2012-12-05	Electronic document
SmartMX2 Crypto Library: User Manual – DES	1.0	2012-12-05	Electronic document
SmartMX2 Crypto Library: User Manual – SHA	1.0	2012-12-05	Electronic document

Name	Release	Date	Form of delivery
SmartMX2 Crypto Library: User Manual – SHA-512	1.0	2012-12-05	Electronic document
SmartMX2 Crypto Library: User Manual – RSA	1.0	2012-12-05	Electronic document
SmartMX2 Crypto Library: User Manual – RSA Key Generation	1.0	2012-12-05	Electronic document
SmartMX2 Crypto Library: User Manual – ECC over GF(p)	1.0	2012-12-05	Electronic document
SmartMX2 Crypto Library: User Manual – Utils	1.0	2012-12-05	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 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.

For the testing performed by the evaluators, the developer has provided a testing environment. The evaluators have reproduced a selection of the developer tests, as well as a small number of test cases designed by the evaluator.

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:

1. A set of card samples (the TOE) containing the following.
   - Hardware sample (P60D080PVC).
   - Cryptographic library loaded into the hardware sample.
   - CryptOS loaded into the hardware sample.
2. A toolset provided by the developer in order to facilitate recreation of the Cryptographic library, and loading the library and the CryptOS 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 Re-used evaluation results

On August 15th, 2012, NXP, the developer of the crypto library submitted an application form to the NSCIB Certification Body requesting to issue a certificate for their Crypto Library V1.0 on P60x080/052/040PVC product.

This security evaluation re-used the evaluation results of the recently performed evaluation of the "Crypto Library V1.0 on P60D024/016/012PVB" (i.e. slightly different hardware platform), certified on February 27th, 2013 under the certification identifier NSCIB-CC-12-36242.

It should be noted that the following Crypto Library – Hardware combinations have been evaluated and certified before:

1. CL v0.9 on P60x144/080PVA certified on December 21st, 2012 under the certification identifier NSCIB-11-31801
2. CL v0.9 on P60x144/080PVA ---> CL v1.0 on P60x144/080PVA certified on January 24th, 2013 under the certification identifier NSCIB-11-31801 (re-issued certificate)
3. CL v0.9 on P60x144/080PVA ---> CL v1.0 on P60D024/016/012PVB certified on February 27th, 2013 under the certification identifier NSCIB-CC-12-36242

The changes between the most recently certified crypto library (Crypto Library V1.0 on the P60D024/016/012PVB) and the Crypto Library V1.0 on the P60x080/052/040PVC (the TOE) can be categorized as[2]:

- **Ø** A slightly different hardware platform.
- **Ø** Developer evidence updates as result of the above changes, including ST and Guidance Documents

The assessment of the update by the evaluation lab in the *[ETR]* indicated that the changes have no security issues and that the original evaluation results could be re-used. For added assurance, minor additional evaluator testing was performed (including perturbation and power and EM side-channel testing, see *[ETRfC]* for details) and developer evidence was analyzed to get sufficient assurance that the changes have no effect on the security level of the TOE).

[2] Differences related to the baseline evaluation (CLv0.9) were handled in their respective evaluations.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number Crypto Library V1.0 on P60x080/052/040PVC. The TOE consists of a hardware part and a software part. This certification covers the configurations of the TOE identified as follows:

The authenticity of the hardware part of the TOE is checked by visual inspection and by reading out the data stored in the memory.

- The die inscription on the surface of the TOE is verified to match the one documented in "Wafer and delivery procedure". Note that there is a minor mistake in the diagram of *[HW-UG-Wafer-3.0]* referred to in the certification report showing the incorrect locations, but correct values, of the identifier. The updated guidance *[HW-UG-Wafer-3.1]* list the same values and the correct locations. The certifier judges that the location of the identifiers has no security impact.
- The data to be read includes the ROM Code Number RCN, the device coding byte DC(1), and the version of the mask VMSK.

The ROM Code Number can be read at address DFFF8Ah. The datasheet *[HW-P60-DATASHEET*] and the platform-ST *[ST-HW]* do not state any requirements for the ROM Code Number. According to the platform-ST, the RCN is "*individual for each customer product*".

Byte DC(1) can be read at address DFFF95h. The values of this parameter, according to *[HW-P60-DATASHEET]*, are for the applicable hardware configurations as follows:

Bits 7 to 0	Type name
0Eh	P60D080
09h	P60D052
0Dh	P60D040
13h	P60C080
15h	P60C052
12h	P60C040

VMSK can be read at address DFFF89h. The platform-ST [HW ST] states that VMSK has to be equal to ASCII "C".

The hardware part of the TOE is identified by P60x080/052/040PVC 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 (as documented in the guidance). The nameplate is specific for the 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.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*[3] 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.

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

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

Security Target		**Pass**

Development		**Pass**
Functional specification	ADV_FSP.5	Pass
Design	ADV_TDS.5	Pass
Implementation representation	ADV_IMP.2	Pass
Internals	ADV_INT.3	Pass
Representation correspondence	ADV_RCR.1	Pass
Security Architecture Description	ADV_ARC.1	Pass
Security Policy Model	ADV_SPM.1	Pass

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

Life cycle support		**Pass**
Advanced Support	ALC_CMC.5	Pass
Development tools CM coverage	ALC_CMS.5	Pass
Delivery procedures	ALC_DEL.1	Pass
Flaw remediation	ALC_FLR.1	Pass
Development security	ALC_DVS.2	Pass
Life cycle definition	ALC_LCD.1	Pass
Tools and techniques	ALC_TAT.3	Pass

Tests		**Pass**
Coverage	ATE_COV.3	Pass
Depth	ATE_DPT.3	Pass
Functional	ATE_FUN.2	Pass
Independent	ATE_IND.2	Pass

Vulnerability assessment		**Pass**
Advanced methodical vulnerability analysis	AVA_VAN.5	Pass

Based on the above evaluation results the evaluation lab concluded the Crypto Library V1.0 on P60x080/052/040PVC to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL 6 augmented by ASE_TSS.2 and ALC_FLR.1**. This implies that the product satisfies the security technical requirements specified in Security Target Crypto Library V1.0 on P60x080/052/040PVC, Rev 1.0, 5 December 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]*.

2.10 Comments/Recommendations

The user guidance as outlined in section 2.5 contains necessary information about the usage of the TOE. Certain aspects of the TOE's security functionality, in particular the countermeasures against attacks, depend on accurate conformance to the user guidance of both the software and the hardware part of the TOE. There are no particular obligations or recommendations for the user apart from following the user guidance. Please note that the documents contain relevant details with respect to the resistance against certain attacks.
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 hardware user guidance.

3 Security Target

The Security Target Crypto Library V1.0 on P60x080/052/040PVC, Rev 1.0, 5 December 2012 is included here by reference.

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.

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

[ETR] Brightsight, Evaluation Technical Report Crypto Library V1.0 on P60x080/052/040PVC EAL6+, 13 -RPT-034 v4.0, dated d.d. July 24, 2013.

[ETRfC] Brightsight, Evaluation Technical Report for Composite Evaluation Crypto Library V1.0 on P60x080/052/040PVC EAL6+, 13 -RPT-035 v5.0, dated July 24, 2013.

[ETR-HW] T-Systems ETR for composite evaluation P60x080/052/040PVC, version 5, 24 April 2013

[HW-CERT] Certification Report. NXP Secure Smart Card Controller P60x080/052/040PVC, BSI-DSZ-CC-0837-2013, June 24, 2013

[HW-P60-DATASHEET] SmartMX family P60D040/052/080 VC Product data sheet, Revision 3.0, 31 October 2012

[HW-UG-Wafer-3.0] Wafer and delivery specification – Rev 3.0, 18 October 2012

[HW-UG-Wafer-3.1] Wafer and delivery specification – Rev 3.1, 8 February 2013

[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 2.1, August 1st, 2011.

[ST] Security Target Crypto Library V1.0 on P60x080/052/040PVC, Rev 1.0, 5 December 2012

[ST-HW] P60x080/052/040PVC Security Target, Revision 1.0, 13 December 2012

(This is the end of this report).