Certification Report

Firmware Libraries V1.1 on P40C012/040/072 VD

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

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

Report number:	**NSCIB-CC-13-37968-CR**
Report version:	**1**
Project number:	**NSCIB-CC-13-37968**
Authors(s):	**Wouter Slegers**
Date:	**March 12th, 2015**
Number of pages:	**16**
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 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 4 (ISO/IEC 15408)

Certificate number **C13-37968**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer

NXP Semiconductors Germany GmbH, Business Unit Security and Connectivity

Stresemannallee 101, D-22529 Hamburg, Germany

Product and assurance level

Firmware Libraries V1.1 on P40C012/040/072 VD

Assurance Package:

- EAL5 augmented with ALC_DVS.2, AVA_VAN.5 and ASE_TSS.2

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-13-37968-CR**

Evaluation facility

Brightsight BV located in Delft, the Netherlands

Applying the Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1 Revision 4 (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 4 for conformance to the Common Criteria for IT Security Evaluation version 3.1 Revision 4. 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 : **12-03-2015**

Certificate expiry : **12-03-2020**

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 as well as for protection profiles and sites.

Part of the procedure is the technical examination (evaluation) of the product, protection profile or site 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 or site complies with the security requirements specified in the associated (site) security target, or that the protection profile (PP) complies with the requirements for PP evaluation specified in the Common Criteria for Information Security Evaluation. A (site) security target is a requirements specification document that defines the scope of the evaluation activities.

The consumer should review the security target or protection profile, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product or site satisfies the security requirements stated in the (site) security target.

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

Recognition of the certificate

Presence of the Common Criteria Recognition Arrangement and SOG-IS logos on the certificate indicates that this certificate is issued in accordance with the provisions of the CCRA and the SOG-IS agreement and will be recognised by the participating nations.

International recognition

The CCRA has been signed by the Netherlands in May 2000 and provides mutual recognition of certificates based on the CC. Starting 8 September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance components up to and including EAL2+ALC_FLR. The current list of signatory nations and approved certification schemes can be found on: http://www.commoncriteriaportal.org.

Certificates issued before 08 September 2014 are still under recognition according to the rules of the previous CCRA (i.e. recognition based on assurance components up to and including EAL4+ALC_FLR). Also certification procedures started before 8 September 2014 and Assurance Continuity (maintenance and re-certification) of old certificates remain recognised according to the rules of the previous CCRA.

The certification of this product has started before 8 September 2014 and thus the recognition of the certificate falls under the recognition rules of the previous CCRA.

European recognition

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 Firmware Libraries V1.1 on P40C012/040/072 VD. The developer of the Firmware Libraries is NXP Semiconductors Germany GmbH, Business Unit Security and Connectivity 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 Firmware Libraries V1.1 on P40C012/040/072 VD) consists of the Firmware Libraries V1.1 and the NXP Secure Smart Card Controller P40C012/040/072 VD. For ease of reading the TOE is often called "SmartMX2 P40 FW Libraries V1.1".

The evaluation of the TOE was conducted as a composite evaluation and uses the results of the CC evaluation of the underlying NXP Secure Smart Card Controller P40C012/040/072 VD certified under the Dutch CC Scheme on 7 October 2014 (*[HW CERT]*).

The SmartMX2 P40 FW Libraries V1.1 is a set of firmware libraries, which provides a set of cryptographic, memory and communications functions that can be used by the Smartcard Embedded Software. The firmware libraries consist 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 ROM. The NXP SmartMX2 P40 smart card processor provides the computing platform and cryptographic support by means of co-processors for the SmartMX2 P40 FW Libraries V1.1.

The Crypto-Library part of the TOE provides AES, DES, Triple-DES (3DES), RSA, 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 P40.

The Crypto-Library part of the TOE also provides a secure copy routine, a secure compare routine and includes internal security measures for residual information protection. For more details refer to the *[ST]*, chapter 1.4.2.

The HAL-Library provides memory functions to operate on RAM and NV memory, functions to compute CRCs, and Config and Patch functionality.

Finally, the Comm-Library part of the TOE provides an interface to the T=0 and T=1 protocols of ISO/IEC 7816-3.

Note that there are no specific security requirements on the functions of the HAL- and Comm-Library, so the memory handling, CRC, Config and Patch functionality, is outside the scope of evaluation.

The TOE has been evaluated by Brightsight B.V. located in Delft, The Netherlands. The evaluation was completed on 5 March 2015 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 scope of the evaluation is defined by the Security Target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the SmartMX2 P40 FW Libraries V1.1, 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 SmartMX2 P40 FW Libraries V1.1 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]* 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), AVA_VAN.5 (Advanced methodical vulnerability analysis) and ASE_TSS.2 (TOE summary specification with architectural design summary).

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4 *[CEM*], for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 4 *[CC*].

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the Firmware Libraries V1.1 on P40C012/040/072 VD 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 Firmware Libraries V1.1 on P40C012/040/072 VD from NXP Semiconductors Germany GmbH, Business Unit Security and Connectivity 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
Hardware platform				
IC hardware	P40C012/040/072 VD	VD	2014-02-06	wafer, module (dice have nameplate 9511D)
IC Dedicated Test Software	Test Software	00h	2014-02-06	Stored in ROM
IC Dedicated Support Software	Boot Software	00h	2014-02-06	Stored in ROM
	HAL Software	00h	2014-02-06	Stored in ROM

Components of the Crypto Library				
Library File	libCryptoLibSymCiphers.a	1.0	11.09.2014	Electronic file
Library File	libCryptoLibSha.a	1.0	11.09.2014	Electronic file
Library File	libCryptoLibRng.a	1.0	11.09.2014	Electronic file
Library File	libCryptoLibRsa.a	1.0	11.09.2014	Electronic file
Library File	libCryptoLibUtils.a	1.0	11.09.2014	Electronic file
Header File	phCryptoLibSymCiphers.h	1.0	11.09.2014	Electronic file
Header File	phCryptoLibSha.h	1.0	11.09.2014	Electronic file
Header File	phCryptoLibRng.h	1.0	11.09.2014	Electronic file
Header File	phCryptoLibRsa.h	1.0	11.09.2014	Electronic file
Header File	phCryptoLibRsa_OAEP.h	1.0	11.09.2014	Electronic file
Header File	phCryptoLibRsa_PSS.h	1.0	11.09.2014	Electronic file
Header File	phCryptoLibUtils_Arith.h	1.0	11.09.2014	Electronic file
Header File	phCryptoLibUtils_MemMgmt.h	1.0	11.09.2014	Electronic file
Components of the TOE (HAL-Lib and Comm-Lib) – UserMode Customer				
DAT File	SystemMode.dat	1.1	18.11.2014	Electronic file
Library File	libHALLibComm.a	1.1	18.11.2014	Electronic file
BCF File	HAL.bcf	1.1	18.11.2014	Electronic file
CFG File	SystemMode_FirewallValues.cfg	1.1	18.11.2014	Electronic file
Header File	phhalComm.h	1.1	18.11.2014	Electronic file
Header File	phhalConf.h	1.1	18.11.2014	Electronic file
Header File	phhalCrc.h	1.1	18.11.2014	Electronic file
Header File	phhalMem.h	1.1	18.11.2014	Electronic file
Header File	phhalMem_AT.h	1.1	18.11.2014	Electronic file
Header File	phhalMem_NV.h	1.1	18.11.2014	Electronic file

Header File	phhalPatch.h	1.1	18.11.2014	Electronic file
Header File	phP4xAppl.h	1.1	18.11.2014	Electronic file
Components of the TOE (HAL-Lib and Comm-Lib) – SystemMode Customer				
Library File	libHalCL.a	1.1	18.11.2014	Electronic file
Library File	libHalMem.a	1.1	18.11.2014	Electronic file
Header File	libHALLibComm.a	1.1	18.11.2014	Electronic file
Header File	phhalComm.h	1.1	18.11.2014	Electronic file
Header File	phhalCrc.h	1.1	18.11.2014	Electronic file
Header File	phhalMem.h	1.1	18.11.2014	Electronic file
Header File	phhalMem_AT.h	1.1	18.11.2014	Electronic file
Header File	phhalMem_NV.h	1.1	18.11.2014	Electronic file
Header File	phhalInit_CryptoLibSetup.h	1.1	18.11.2014	Electronic file
Header File	phhalInit_ATSetup.h	1.1	18.11.2014	Electronic file
Components of the TOE (HAL-Lib and Comm-Lib) - SystemMode Customer without libHalMem.a				
Library File	libHalCL.a	1.1	18.11.2014	Electronic file
Library File	libHALLibComm.a	1.1	18.11.2014	Electronic file
Header File	phhalComm.h	1.1	18.11.2014	Electronic file
Header File	phhalCrc.h	1.1	18.11.2014	Electronic file
Header File	phhalMem.h	1.1	18.11.2014	Electronic file
Header File	phhalMem_AT_Minimal.h	1.1	18.11.2014	Electronic file
Header File	phhalMem_NV.h	1.1	18.11.2014	Electronic file
Header File	phhalInit_CryptoLibSetup.h	1.1	18.11.2014	Electronic file

To ensure secure usage a set of guidance documents is provided together with the SmartMX2 P40 FW Libraries V1.1. Details can be found in section 2.5 of this report.

The hardware part of the TOE is delivered by NXP together with the IC Dedicated Support Software. The Firmware Libraries are delivered in Phase 1 of the TOE lifecycle (for a detailed and precise description of the TOE lifecycle refer to the *[ST]*, chapter 1.2.2.) 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 Firmware Libraries 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 symmetrical cryptographic algorithms AES, DES and Triple-DES (3DES), in ECB, CBC, CBC-MAC and CMAC modes. The TOE provides the asymmetrical cryptographic algorithm RSA, for signature generation, signature verification, message encoding and signature encoding. RSA public key computation is also provided. The TOE provides the hash algorithms SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512, 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, as well as perturbation 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 provides a secure copy routine and a secure compare routine and includes internal security measures for residual information protection.

Note that the memory handling, CRC, Config and Patch functionality is outside the scope of evaluation.

Note also 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 4.

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, as well as a HAL-Library and a Comm-Library that can be used by the Smartcard Embedded Software. The Libraries consist 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 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 or functions provided.

2.5 Documentation

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

Type	Name	Release	Date	Form of delivery
Hardware platform				
Document	Product data sheet SmartMX2 P40 family P40C012/040/072, Secure high performance smart card controller, NXP Semiconductors	262923	2014-06-27	Electronic document

Document	Product data sheet addendum SmartMX2 P40 family P40Cxxx, Firmware interface specification, NXP Semiconductors	275823	2014-06-27	Electronic document
Document	Product data sheet addendum SmartMX2 P40 family P40Cxxx, User Mode, NXP Semiconductors	275722	2014-06-27	Electronic document
Document	Product data sheet addendum SmartMX2 P40 family P40Cxxx, System Mode, NXP Semiconductors	267522	2014-06-27	Electronic document
Document	Product data sheet addendum SmartMX2 P40 family P40Cxxx, Chip Health Mode, NXP Semiconductors	269720	2014-05-21	Electronic document
Document	Product data sheet addendum SmartMX2 P40 family P40Cxxx, Post Delivery Configuration, NXP Semiconductors	269620	2014-05-21	Electronic document
Document	Product data sheet addendum SmartMX2 P40 family P40Cxxx, Instruction Set Manual, NXP Semiconductors	258121	2014-06-27	Electronic document
Document	Product data sheet addendum SmartMX2 P40 family P40Cxxx VA and VD, Wafer specification, NXP Semiconductors	269822	2014-06-03	Electronic document
Document	Guidance and Operation Manual NXP Secure Smart Card Controller P40C012/040/072, Information on Guidance and Operation, NXP Semiconductors	269422	2014-06-27	Electronic document

Firmware Libraries				
Document	User guidance manual Firmware Libraries V1.1 on P40C012/040/072 VD, Preparative procedures and operational user guidance	1.4	19.12.2014	Electronic document
Document	Product data sheet addendum: SmartMX2 P40 family P40Cxxx HAL Interface Specification	2.4	21.11.2014	Electronic document
Document	User Guidance: Symmetric Crypto Library	1.4	16.10.2014	Electronic document
Document	User Guidance: SHA Library	1.4	16.10.2014	Electronic document
Document	User Guidance: RNG Library	1.5	19.12.2014	Electronic document
Document	User Guidance: RSA Library	1.4	16.10.2014	Electronic document
Document	User Guidance: Utils Library	1.4	16.10.2014	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

Testing by both the developer and evaluator was performed on the Soft Masking Device version of the TOE, which was analysed by the evaluation lab and was concluded to be applicable to all hardware variations of the TOE.

The developer did 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 industry standard and proprietary test suites. 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, as the hardware 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 devised after performing an Evaluator Vulnerability Analysis. This was done in the following steps.

1. Inventory of required resistance
   This step used the JIL attack list *[JIL]* as a reference for completeness and studied the ST claims to decide which attacks in the JIL attack list applied for the TOE, as well as adding the evaluator's proprietary attack knowledge.
2. Validation of security functionalities
   This step identified the implemented security functionalities and performed evaluator independent tests to verify implementation and to validate proper functioning of the security functions.
3. Vulnerability analysis
   In this step the design and the implementation of the security functionalities was studied and an analysis was performed to determine whether the implementation potentially could be vulnerable against the attacks of step 1. Based on this analysis the evaluators determined whether the design and implementation provide sufficient assurance or whether penetration testing is needed to provide sufficient assurance.
4. Penetration testing
   This step performed the penetration tests identified in step 3.
5. Conclusions on resistance
   This step performed a *[JIL]* compliant rating on the results of the penetration tests in relation with the assurance already gained by the design analysis. Based on the ratings the evaluators made conclusions on the resistance of the TOE against attackers possessing a high attack potential.
6. With the maintenance of the hardware, these steps were revisited and a gap analysis was made, leading to additional analysis and tests.

2.6.3 Test Configuration

Testing by the evaluator was performed on the P40C72 V0D, which was analysed by the evaluation lab and was concluded to be applicable to all hardware variations of the TOE.

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 Firmware Libraries' functionality. The test OS, and its documentation, was provided to the evaluators, and was used in all the testing. See the *[ETR]* for details.

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

No direct re-use has been made of previous evaluation results. Indirectly gained knowledge from evaluations of other similar TOEs has been used.

There has been extensive re-use of the ALC aspects for the sites involved in the software component of the TOE (NXP Semiconductors Gratkorn, NXP Semiconductors Hamburg, NXP Semiconductors

Leuven, NXP India Private Limited, D&F Hamburg). Sites involved in the development and production of the hardware platform were re-used by composition.

No sites have been visited as part of this evaluation.

2.8 Evaluated Configuration

The TOE is defined uniquely by its name and version number "Firmware Libraries V1.1 on P40C012/040/072 VD". 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 [HW UG-Wafer].
- The data to be read by using phhalSystem_GetVersion. The bytes *v* and *eee* in particular contain the TOE information as shown in the following table.

Bytes	Value	Meaning
V	0x18h	P40C VD
Eee	0x0Dh	P40C012
	0x28h	P40C040
	0x48h	P40C072

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]*[1] 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 al claimed assurance requirements is: **Pass**

Based on the above evaluation results the evaluation lab concluded the Firmware Libraries V1.1 on P40C012/040/072 VD to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements of **EAL5 augmented with ALC_DVS.2, AVA_VAN.5 and ASE_TSS.2**. This implies that the product satisfies the security technical requirements specified in Firmware Libraries V1.1 on P40C012/040/072 VD Security Target, Revision 1.6, January 09, 2015.

The Security Target claims 'strict conformance' to the Protection Profile *[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.

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

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 Firmware Libraries must implement the advices of the hardware user guidance.

Note that the memory handling, CRC, Config and Patch functionality is outside the scope of evaluation.

3 Security Target

The Security Target *[ST]* is included here by reference. Please note that for the need of publication a public version of the Security Target *[ST-lite]* 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, II and III, version 3.1 Revision 4.

[CEM] Common Methodology for Information Technology Security Evaluation, version 3.1, Revision 4.

[ETR] ETR Firmware Libraries V1.1 on P40C012/040/072 VD EAL5+, Document reference 15-RPT-034, version 1.0, dated 2015-02-23

[ETRfC] ETR for Composite Evaluation Firmware Libraries V1.1 on P40C012/040/072 VD EAL5+, Document reference 15-RPT-025, version 2.0, dated 2015-02-23

[ETR-HW] Evaluation Technical Report for Composition NXP Secure Smart Card Controller P40C012/040/072 VD EAL5+, Revision 1.0, 29 September 2014

[HW CERT] Certification Report NXP Secure Smart Card Controller P40C012/040/072 VD, Revision 1.0, 07 October 2014

[HW-UG-Wafer] Product data sheet addendum SmartMX2 P40 family P40Cxxx VA and VD, Wafer specification, NXP Semiconductors, 269822, dated 2014-06-03

[JIL] Attack methods for Smart cards and similar devices, JIL, version 2.9, January 2013.

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.1, August 1st, 2011.

[ST] Firmware Libraries V1.1 on P40C012/040/072 VD Security Target, Revision 1.6, January 09, 2015

[ST LITE] Firmware Libraries V1.1 on P40C012/040/072 VD Security Target Lite, Revision 1.1, 09 January 2015

[ST-HW] NXP Secure Smart Card Controller P40C012/040/072 VD Security Target, Revision 1.4, 25 September 2014

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

(This is the end of this report).