TÜV Rheinland Nederland B.V.

Certification Report

Firmware Libraries V2.x on P40C008/012/024/040/072 VE.001

Sponsor and developer:	***NXP Semiconductors GmbH, Business Unit Security & Connectivity*** **Stresemannallee 101** **D-22529 Hamburg** **Germany**
Evaluation facility:	***Brightsight*** **Delftechpark 1** **2628 XJ Delft** **The Netherlands**
Reportnumber:	**NSCIB-CC-65156-CR2**
Report version:	**2**
Projectnumber:	**65156**
Author:	**Wouter Slegers**
Date:	**26 July 2017**
Number of pages:	**16**
Number of appendices:	**0**

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

Headoffice:
Westervoortsedijk 73
NL-6827 AV Arnhem

P.O. Box 2220
NL-6802 CE Arnhem
The Netherlands

Location Leek:
Eiberkamp 10
NL-9351 VT Leek

P.O. Box 37
NL-9350 AA Leek
The Netherlands

info@nl.tuv.com
www.tuv.com/nl

Tel. +31 (0)88 888 7 888
Fax +31 (0)88 888 7 879

TÜV Rheinland Nederland B.V. is a registered company at the Dutch Chamber of Commerce under number 27288788

VAT number: NL815820380B01
IBAN: NL61DEUT0265155096

Certificate

Standard

Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 Revision 4 (ISO/IEC 15408)

Certificate number **CC-17-65156**

TÜV Rheinland Nederland B.V. certifies:

Certificate holder and developer

NXP Semiconductors GmbH,
Business Unit Security & Connectivity

Stresemannallee 101, D-22529 Hamburg, Germany

Product and assurance level

Firmware Libraries V2.x on P40C008/012/024/040/072 VE.001

Assurance Package:

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

Protection Profile Conformance:

- Security IC Platform Protection Profile with Augmentation Packages, registered under the reference BSI-PP-0084-2014, version 1.0, 13.01.2014. No Augmentation Packages used.

Project number **NSCIB-CC-65156**

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 EAL2

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.

SOGIS IT SECURITY CERTIFIED

SOGIS Mutual Recognition Agreement for components up to EAL7

Validity

Date of 1st issue : **22-12-2015**
Date of re-issue : **27-07-2017**
Certificate expiry : **22-12-2020**

PRODUCTS
RvA C 078
Accredited by the Dutch Council for Accreditation

TÜV Rheinland Nederland B.V.
P.O. Box 2220
NL-6802 CE Arnhem
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 (site) 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 IT product's 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 would indicate 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 September 2014 the CCRA has been updated to provide mutual recognition of certificates based on cPPs (exact use) or STs with evaluation assurance levels 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.

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 V2.x on P40C008/012/024/040/072 VE.001. The developer of the Firmware Libraries V2.x on P40C008/012/024/040/072 VE.001 is NXP Semiconductors GmbH, Business Unit Security & 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 V2.x on P40C008/012/024/040/072 VE.001) consists of the Firmware Libraries V2.x and the NXP Secure Smart Card Controller P40C008/012/024/040/072 VE.001. For ease of reading the TOE is often called "SmartMX2 P40 FW Libraries V2.x". *Currently only the version where x=0.1 is supported.*

The Firmware Libraries V2.x on P40C008/012/024/040/072 VE.001 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 Firmware Libraries V2.x on P40C008/012/024/040/072 VE.001.

The Crypto-Library part of the TOE provides DES, Triple-DES (3DES), RSA, RSA Key Generation, ECDA, 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 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.

The TOE has been originally evaluated by Brightsight B.V. located in Delft, The Netherlands and was certified on 22 December 2015 and maintained on 2 June 2016. The re-evaluation of the TOE also took place by Brightsight B.V. and was conducted as a composite evaluation reusing the results of the CC evaluation of the underlying NXP Secure Smart Card Controller P40C008/012/024/040/072 VE.001 certified under the Dutch CC Scheme on 04 May 2017 (*[HW CERT]*). The re-evaluation was completed on 25 July 2017 with the approval of the ETR.

The re-certification procedure has been conducted in accordance with the provisions of the Netherlands Scheme for Certification in the Area of IT Security *[NSCIB]*.

This second issue of the Certification Report is a result of a "recertification with major changes".

The major changes are reduction of variants of the Secure Smart Card Controller (i.e. the underlying VD hardware and the VE hardware with 000 software are no longer included) and exclusion of the AES functionality from the evaluation scope.

Small changes to the Crypto Library's guidance are also included. No changes to the implementation details of the Crypto Library itself have been made.

The security evaluation re-used the evaluation results of previously performed evaluations. A full, up to date vulnerability analysis has been made, as well as renewed testing.

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

Note that the Firmware libraries v1.0 included the Comm-library in the TOE scope, the Firmware libraries v2.0 and v2.x (where x=0.1) do not.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the Firmware Libraries V2.x on P40C008/012/024/040/072 VE.001, 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 Firmware Libraries V2.x on P40C008/012/024/040/072 VE.001 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), ASE_TSS.2 (TOE summary specification with architectural design summary), 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 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 V2.x on P40C008/012/024/040/072 VE.001 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.

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

2 Certification Results

2.1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this evaluation is the Firmware Libraries V2.x on P40C008/012/024/040/072 VE.001 from NXP Semiconductors GmbH, Business Unit Security & Connectivity located in Hamburg, Germany.

The TOE is comprised of the following main components:

Type	Name	Release	Date	Form of delivery
Hardware platform				
IC hardware	P40C008/012/024/040/072 VE	VE	2015-02-16	wafer, module (dice have nameplate 9511E)
IC Dedicated Test Software	Test Software	01h	2017-03-01	in ROM
IC Dedicated Support Software	Boot Software	01h	2017-03-01	in ROM
	HAL Software	01h	2017-03-01	in ROM
Components of the Crypto Library				
Library File	libCryptoLibSymCiphers.a	2.0	17.09.2015	Electronic file
Library File	libCryptoLibSha.a	2.0	17.09.2015	Electronic file
Library File	libCryptoLibRng.a	2.0	17.09.2015	Electronic file
Library File	libCryptoLibRsa.a	2.0	17.09.2015	Electronic file
Library File	libCryptoLibUtils.a	2.0	17.09.2015	Electronic file
Library File	libCryptoLibUtils_ImportExport.a	2.0	17.09.2015	Electronic file
Library File	libCryptoLibRsaKg.a	2.0	17.09.2015	Electronic file
Library File	libCryptoLibEccGfp.a	2.0	17.09.2015	Electronic file
Header File	phCryptoLibSymCiphers.h	2.0	17.09.2015	Electronic file
Header File	phCryptoLibSha.h	2.0	17.09.2015	Electronic file
Header File	phCryptoLibRng.h	2.0	17.09.2015	Electronic file
Header File	phCryptoLibRsa.h	2.0	17.09.2015	Electronic file
Header File	phCryptoLibRsa_OAEP.h	2.0	17.09.2015	Electronic file
Header File	phCryptoLibRsa_PSS.h	2.0	17.09.2015	Electronic file
Header File	phCryptoLibUtils_Arith.h	2.0	17.09.2015	Electronic file
Header File	phCryptoLibUtils_MemMgmt.h	2.0	17.09.2015	Electronic file
Header File	phCryptoLibRsaKg.h	2.0	17.09.2015	Electronic file
Header File	phCryptoLibEccGfp.h	2.0	17.09.2015	Electronic file
Components of the HAL Library – UserMode Customer				
DAT File	SystemMode.dat	1.2.1	25.01.2016	Electronic file
BCF File	HAL.bcf	1.2.1	25.01.2016	Electronic file
CFG File	SystemMode_FirewallValues.cfg	1.2.1	25.01.2016	Electronic file
Header File	phhalConf.h	1.2.1	25.01.2016	Electronic file
Header File	phhalCrc.h	1.2.1	25.01.2016	Electronic file
Header File	phhalMem.h	1.2.1	25.01.2016	Electronic file
Header File	phhalMem_AT.h	1.2.1	25.01.2016	Electronic file

Header File	phhalMem_NV.h	1.2.1	25.01.2016	Electronic file
Header File	phhalPatch.h	1.2.1	25.01.2016	Electronic file
Header File	phP4xAppl.h	1.2.1	25.01.2016	Electronic file
Components of the HAL Library – SystemMode Customer				
Library File	libHalCL.a	1.2.1	25.01.2016	Electronic file
Library File	libHalMem.a	1.2.1	25.01.2016	Electronic file
Header File	phhalCrc.h	1.2.1	25.01.2016	Electronic file
Header File	phhalMem.h	1.2.1	25.01.2016	Electronic file
Header File	phhalMem_AT.h	1.2.1	25.01.2016	Electronic file
Header File	phhalMem_NV.h	1.2.1	25.01.2016	Electronic file
Header File	phhalInit_CryptoLibSetup.h	1.2.1	25.01.2016	Electronic file
Header File	phhalInit_ATSetup.h	1.2.1	25.01.2016	Electronic file
Components of the HAL library - SystemMode Customer without libHalMem.a				
Library File	libHalCL.a	1.2.1	25.01.2016	Electronic file
Header File	phhalCrc.h	1.2.1	25.01.2016	Electronic file
Header File	phhalMem.h	1.2.1	25.01.2016	Electronic file
Header File	phhalMem_AT_Minimal.h	1.2.1	25.01.2016	Electronic file
Header File	phhalMem_NV.h	1.2.1	25.01.2016	Electronic file
Header File	phhalInit_CryptoLibSetup.h	1.2.1	25.01.2016	Electronic file

To ensure secure usage a set of guidance documents is provided together with the Firmware Libraries V2.x on P40C008/012/024/040/072 VE.001. 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 DES and Triple-DES (3DES), in ECB, CBC, CBC-MAC and CMAC modes.

The TOE provides the asymmetrical cryptographic algorithms RSA, for signature generation, signature verification, message encoding and signature encoding. RSA key generation and RSA public key computation is also provided.

The TOE provides the asymmetrical cryptographic algorithm ECDSA, for signature generation and signature verification. ECDSA key generation, ECDH key exchange and secure point multiplication and addition over Elliptic Curves over GF(p) are 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. 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 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 objectives for the environment are of relevance:

- OE.Resp-Appl: Treatment of User Data
- OE.Process-Sec-IC: Protection during composite product manufacturing
- OE.Check-Init: Check of initialization data by the Security IC Embedded Software

Details can be found in the Security Target *[ST]* sections 4.2 and 4.3.

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.

Note that there are no longer specific security requirements on AES, so the AES functionality is outside the scope of evaluation.

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

Note that the Firmware libraries v1.0 included the Comm-library in the TOE scope, the Firmware libraries v2.0 and v2.x (where x=0.1) do not.

Composite product developers should do their own security analysis and/or testing.

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 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 P40C008/012/024/040/072, Secure high-performance smart card controller, NXP Semiconductors	262936	2017-02-16	Electronic document
Document	Product data sheet addendum SmartMX2 P40 family P40Cxxx, Firmware interface specification, NXP Semiconductors	275836	2017-03-10	Electronic document
Document	Product data sheet addendum SmartMX2 P40 family P40Cxxx, User Mode, NXP Semiconductors	275733	2016-06-17	Electronic document
Document	Product data sheet addendum SmartMX2 P40 family P40Cxxx, System Mode, NXP Semiconductors	267531	2016-06-17	Electronic document
Document	Product data sheet addendum SmartMX2 P40 family P40Cxxx, Chip Health Mode, NXP Semiconductors	269730	2015-04-01	Electronic document
Document	Product data sheet addendum SmartMX2 P40 family P40Cxxx, Post Delivery Configuration, NXP Semiconductors	269630	2015-04-01	Electronic document
Document	Product data sheet addendum SmartMX2 P40 family P40Cxxx, Instruction Set Manual, NXP Semiconductors	258132	2015-06-26	Electronic document
Document	Product data sheet addendum SmartMX2 P40 family P40Cxxx VA, VD and VE, Wafer specification, NXP Semiconductors	269832	2015-05-30	Electronic document
Document	Guidance and Operation Manual NXP Secure Smart Card Controller P40C008/012/024/040/072, Information on Guidance and Operation, NXP Semiconductors	269433	2017-02-24	Electronic document
Components of the Crypto Library				
Document	User guidance manual Firmware Libraries V2.x on P40C008/012/024/040/072 VE.001, Preparative procedures and operational user guidance	0.9	09.05.2017	Electronic document
Document	User Guidance: Symmetric Crypto Library	1.6	11.11.2015	Electronic document
Document	User Guidance: SHA Library	1.6	11.11.2015	Electronic document
Document	User Guidance: RNG Library	1.9	11.11.2015	Electronic document
Document	User Guidance: RSA Library	1.6	11.11.2015	Electronic document
Document	User Guidance: Utils Library	1.6	11.11.2015	Electronic document
Document	User Guidance: RSA Key Generation Library	0.3	11.11.2015	Electronic document
Document	User Guidance: ECC over GF(p) Library	0.3	11.11.2015	Electronic document
Components of the HAL Library – UserMode Customer				
Document	User guidance manual Firmware Libraries V2.x on P40C008/012/024/040/072 VE.001, Preparative procedures and operational user guidance	0.9	09.05.2017	Electronic document
Document	Product data sheet addendum: SmartMX2 P40 family P40Cxxx HAL Interface Specification	3.2	16.11.2015	Electronic document
Components of the HAL Library – SystemMode Customer				
Document	User guidance manual Firmware Libraries V2.x on P40C008/012/024/040/072 VE.001, Preparative procedures and operational user guidance	0.9	09.05.2017	Electronic document
Document	Product data sheet addendum: SmartMX2 P40 family P40Cxxx HAL Interface Specification	3.2	16.11.2015	Electronic document
Components of the HAL library - SystemMode Customer without libHalMem.a				
Document	User guidance manual Firmware Libraries V2.x	0.9	09.05.2017	Electronic document

	on P40C008/012/024/040/072 VE.001, Preparative procedures and operational user guidance			
Document	Product data sheet addendum: SmartMX2 P40 family P40Cxxx HAL Interface Specification	3.2	16.11.2015	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 TOE and on a Soft Masking Device version of the TOE. This was analysed by the evaluation lab and was concluded to be applicable to all hardware variations of the TOE.

The developer has performed extensive testing on functional specification, 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.

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 re-certification of the TOE is done by performing a new vulnerability assessment according to the latest security standards. The vulnerability of the TOE for these attacks has been analysed in a white box investigation conforming to AVA_VAN.5.

1. *Inventory of required resistance*
   The reference for attack techniques against which smart card-related devices controllers such as the TOE must be protected against is the document "Attack methods for smart cards" *[JIL-AM]*. Also the Brightsight attack lists for several algorithms have been used, and Brightsight's latest improvements in evaluation techniques have been considered.

2. *Validation of security functionalities*
   This step identifies the implemented security functionalities and performs tests to verify the implementation and to validate proper functioning. This step has been performed as a part of the ATE evaluation; the ATE results of the baseline certification have been reused for this certification.

3. *Vulnerability analysis*
   This step first gives an overview against which attacks the implemented security functionalities are meant to provide protection. Secondly in this step the design of the implemented security functionalities is studied. Thirdly, an analysis is performed to determine whether the design contains vulnerabilities against the respective attacks of step 1.

   The results of the vulnerability analysis are presented in the combined first meeting, including the test plan, and have been updated based on comments and input from the scheme.

4. *Analysis of input from other evaluation activities*
   The *[ST]* has been updated since the previous evaluation. The new version has been evaluated. The results of the evaluation are presented in an updated ASE intermediate report. The user guidance and the hardware documentation has been updated as well. The changes and their impact have been analysed in a gap analysis.

5. *Design assurance evaluation*
   This step analyses the results from an attack perspective as defined in Step 3. Based on this design analysis the evaluators determine whether the design provides sufficient assurance or whether penetration testing is needed to provide sufficient assurance.

6. *Penetration testing*
   This step performs the penetration tests identified in Step 3.
7. *Conclusions on resistance*
   This step performs a *[JIL-AM]* 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 draw conclusions on the resistance of the Firmware Libraries against attackers possessing a high attack potential.

2.6.3 Test Configuration

Testing by the evaluator was performed on the P40C072 V0E, which was analysed by the evaluation lab and was concluded to be applicable to all hardware variations of the TOE, including the VE.001.

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.

The algorithmic security level of cryptographic functionality has not been rated in this certification process, but the current consensus on the algorithmic security level in the open domain, i.e. from the current best cryptanalytic attacks published, has been taken into account.

The algorithmic security level exceeds 100 bits for all evaluated cryptographic functionality as required for high attack potential (AVA_VAN.5). Note that the algorithmic attack on two key 3DES is considered impractical for these kind of products.

The strength of the implementation of the cryptographic functionality has been assessed in the evaluation, as part of the AVA_VAN activities. These activities revealed that for some cryptographic functionality the security level could be reduced. As the remaining security level still exceeds 100 bits, this is considered sufficient. So no exploitable vulnerabilities were found with the independent penetration tests.

For composite evaluations, please consult the *[ETRfC]* for details.

2.7 Re-used evaluation results

This is a re-certification: direct re-use has been made of the previous evaluation results on the same hardware platforms with slightly updated firmware. Verification has been performed to verify that the newer VE.001 firmware of the hardware platforms has no impact on the results with the older firmware.

There has been extensive re-use of the ALC aspects for the sites involved in the software component of the TOE NXP Semiconductors Eindhoven HTC60, 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 V2.x on P40C008/012/024/040/072 VE.001 where x=0.1.

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

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]*[2] which references the ASE Intermediate Report 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 "**Pass**".

Based on the above evaluation results the evaluation lab concluded the Firmware Libraries V2.x on P40C008/012/024/040/072 VE.001, to be **CC Part 2 extended, CC Part 3 conformant**, and to meet the requirements **of EAL 5 augmented with ALC_DVS.2, ASE_TSS.2 and AVA_VAN.5**. This implies that the product satisfies the security technical requirements specified in Security Target *[ST]*.

The Security Target claims strict conformance to the Protection Profile *[PP-0084]*. No Augmentation Packages from the PP have been used.

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).

Note that there are no longer specific security requirements on AES, so the AES functionality is outside the scope of evaluation.

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

Note that the Firmware libraries v1.0 included the Comm-library in the TOE scope, the Firmware libraries v2.0 and v2.x (where x=0.1) do not.

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

3 Security Target

The Firmware Libraries V2.x on P40C008/012/024/040/072 VE.001 Security Target, Rev. 0.9, 9 May 2017 *[ST]* is included here by reference.

Please note that for the need of publication a public version (Firmware Libraries V2.x on P40C008/012/024/040/072 VE.001 Security Target Lite, Revision 1.3, 9 May 2017) *[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:

AES	Advanced Encryption Standard
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)
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
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
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:

[CC] Common Criteria for Information Technology Security Evaluation, Parts I, II and III, Version 3.1 Revision 4, September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.

[ETR] ETR NXP Firmware Libraries V2.x on P40C008/012/024/040/072 VE.001 EAL5+, document reference 17-RPT-273, version 4.0, dated 23 June 2017

[ETRfC] ETR for Composition NXP Firmware Libraries V2.x on P40C008/012/024/040/072 VE.001 EAL5+, document reference 17-RPT-315, version 2.0, dated 27 June 2017

[HW-CERT] Certification Report NXP P40C008/012/024/040/072 VE.001, Revision 2, 3 May 2017

[HW-ETRfC] Brightsight, Evaluation Technical Report for Composition NXP Secure Smart Card Controller P40C008/012/024/040/072 VE.001 EAL5, 17-RPT-137 v3.0, dated 03 May 2017.

[HW-ST] NXP Secure Smart Card Controller P40C008/012/024/040/072 VE.001 Security Target, Rev. 2.2, 10 March 2017

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.2, August 10th, 2015.

[PP-0084] Security IC Platform Protection Profile with Augmentation Packages", reference BSI-CC-PP-0084-2014, version 1.0, 13.01.2014.

[ST] Firmware Libraries V2.x on P40C008/012/024/040/072 VE.001 Security Target, Rev. 0.9, 09. May 2017.

[ST-lite] Firmware Libraries V2.x on P40C008/012/024/040/072 VE.001 Security Target Lite, Revision 1.3, 9 May 2017

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

(This is the end of this report).