Certification Report

NXP Secure Smart Card Controller P40C008/012/024/040/072 VE.001

Sponsor and developer: ***NXP Semiconductors GmbH, Business Unit Security & Connectivity***
Stresemannallee 101
22505 Hamburg
Germany

Evaluation facility: ***Brightsight B.V***
Brassersplein 2
2612 CT Delft
The Netherlands

Report number:	**NSCIB-CC-0262848-CR**
Report version:	**1**
Project number:	**0262848**
Author(s):	**Wouter Slegers**
Date:	**12 February 2021**
Number of pages:	**13**
Number of appendices:	**0**

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

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.

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 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.

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 NXP Secure Smart Card Controller P40C008/012/024/040/072 VE.001. The developer of the NXP Secure Smart Card Controller 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) is a hardware secure smart card controller with IC Dedicated software. A Smartcard Embedded Software developer may create Security IC Embedded Software to execute on the NXP Secure Smart Card Controller P40C008/012/024/040/072 VE.001 hardware. This software is stored in arbitrary memory of the NXP Secure Smart Card Controller P40C008/012/024/040/072 VE.001 hardware and is not part of the TOE.

The TOE provides a hardware co-processor for Triple-DES (3DES) and AES (not in the evaluated scope), an AIS31-compliant True Random Number Generator (TRNG), a memory management unit (MMU) for access control management and ISO/IEC 7816 contact interface with UART.

The TOE also contains IC Dedicated software which provides support functionalities such as basic NVM access, Post-Delivery Configuration feature, self-testing, error counter handling and TOE reset.

The TOE has been originally evaluated by Brightsight B.V. located in Delft, The Netherlands and was certified on 18 August 2015 under the certification ID NSCIB-CC-13-37658, and re-certified under the certification ID NSCIB-CC-65655, first on 18 August 2015 and again on 3 May 2017,. This re-evaluation also took place by Brightsight B.V. and was completed on 12 February 2021 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]*.

For procedural reasons, this certification is a new certification.

There are no changes between the NSCIB-CC-65655-CR2 and this certification scope.

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.

The scope of the evaluation is defined by the security target *[ST]*, which identifies assumptions made during the evaluation, the intended environment for the NXP Secure Smart Card Controller 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 NXP Secure Smart Card Controller 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 provides sufficient evidence that the TOE 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 5 and *[CEM]* for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 5 *[CC]* (Parts I, II and III).

TÜV Rheinland Nederland B.V., as the NSCIB Certification Body, declares that the 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 NXP Secure Smart Card Controller 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:

Delivery item type	Identifier	Version
Hardware	P40C008/012/024/040/072	VE.001
Software	Test Software	01h
	Boot software	01h
	HAL Software	01h

To ensure secure usage a set of guidance documents is provided together with the NXP Secure Smart Card Controller P40C008/012/024/040/072 VE.001. Details can be found in section 2.5 of this report.

The TOE is delivered by NXP as a wafer in phase 3 or in packaged form in phase 4 of the smart card life cycle as defined in the Smart Card IC Protection Profile *[PP-0084]*. Security IC Embedded Software (not part of the TOE) can be loaded in ROM in Phase 3.

2.2 Security Policy

A Security IC must provide high security in particular when being used in the banking and finance market, in electronic commerce or in governmental applications.

Hence the TOE shall maintain:

- the integrity and confidentiality of code and data stored in its memories,
- the different CPU modes with the related capabilities for configuration and memory access,
- the integrity, the correct operation and the confidentiality of security functionality provided by the TOE.

This is ensured by the construction of the TOE and its security functionality.

The NXP Secure Smart Card Controller P40C008/012/024/040/072 VE.001.basically provides a hardware platform for an implementation of a smart card application with:

- functionality to calculate Data Encryption Standard (Triple-DES) with up to three keys,
- a True Random Number Generator,
- memory management control, and
- an ISO/IEC 7816 contact interface with UART.

In addition, several security mechanisms are implemented to ensure proper operation as well as integrity and confidentiality of stored data. For example, this includes security mechanisms for memory protection and security exceptions as well as sensors, which allow operation under specified conditions only. Memory encryption is used for memory protection and chip shielding is added to the chip.

Hardware support to calculate Advanced Encryption Standard (AES) with different key lengths, large integer arithmetic operations like multiplication, addition and logical operations, which are suitable for public key cryptography and elliptic curve cryptography, as well as support for cyclic redundancy

check (CRC) calculation, is functionally in the TOE, however not part of the claimed security functionality.

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. Detailed information on these security objectives that must be fulfilled by the TOE environment can be found in section 4.2 and 4.3 of the *[ST]*.

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.

Please note that although the TOE contains accelerators for AES, CRC and large number arithmetic, the functionality and security of these features has not been topic of this evaluation. Composite product developers should do their own security analysis and/or testing.

2.4 Architectural Information

The target of evaluation (TOE) is a Security IC with Dedicated Test Software and Dedicated Support Software.

The TOE does not include any Security IC Embedded Software. See *[ST]* section 1.4 for details.

2.5 Documentation

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

Type	Name	Release	Date	Form of delivery
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

Type	Name	Release	Date	Form of delivery
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

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

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.

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 evaluator has not repeated the developer tests, but found the tests to be identical to the tests of the baseline evaluations. As implementation remains unchanged between the previous certified TOE, no tests have been added for this re-certification.

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 implementation and to validate proper functioning. This step has been performed as part of ATE evaluation, and was fully re-used from the previous re-certification of the TOE.

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 CC re-certification is done in parallel with an EMVCo renewal for this TOE. Both activities are performed within Brightsight, and the same vulnerability analysis is used for both, the EMVCo renewal, and the CC re-certification with regards to the claims made for this TOE, and where the TOE scope allows for it.

The results of the vulnerability analysis are presented to the certifier in a meeting, including the test plan, and have been updated based on comments and input from the scheme. This step has been performed as part of AVA evaluation.

4. *Analysis of input from other evaluation activities*

   During the course of the evaluation the developer decided to modify the TOE, which resulted in an update of the *[ST]*. The updated *[ST]* was evaluated and taken along as input in the AVA evaluation and was found not to affect other CC classes.

5. *Design assurance evaluation*

   This step analyses the results from an attack perspective as defined in step 1. Based on this design analysis the evaluators determine whether the design provides sufficient assurance or whether penetration testing is needed to provide sufficient assurance. This step has been performed as part of AVA evaluation.

6. *Penetration testing*

   This step performs the penetration tests identified in step 3. This step has been performed as part of AVA evaluation.
   Note that tests have been performed on a sample that is slightly different from the actual TOE. The difference is in a part that is only accessed in test mode, which is not accessible or available to the end user, and is extensively analysed. The results of this analysis have been presented to the certifier in a meeting.

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 TOE against attackers possessing a high attack potential. This step has been performed as part of AVA evaluation.

The total test effort expended by the evaluators was 8 weeks. During that test campaign 0% of the total time was spend on Perturbation attacks, 100% on side channel testing and 0% on logical tests

2.6.3 Test Configuration

Testing was performed on the TOE in the 072 configuration.

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.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 "high attack potential".

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 from an algorithmic security level above 100 bits to a practical remaining security level lower than 100 bits. As the remaining security level still exceeds 80 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 formally a new certification but effectively a re-certification. Documentary evaluation results of the earlier version of the TOE have been re-used, but vulnerability analysis and penetration testing has been renewed.

There has been extensive re-use of the ALC aspects for the sites involved in the development and production of the TOE, by use of 14 site certificates.

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 NXP Secure Smart Card Controller P40C008/012/024/040/072 VE.001.

All major configurations as well as all minor configuration options that can be selected are described in chapter 1.4.2 of the *[ST]*. All major and minor configurations are available to the evaluator. Besides the size of the available EEPROM memory, there are no differences between the major configurations. The major configurations do not have dependencies to security features. All minor configuration options that are part of the evaluation were tested and behave as specified.

Therefore the results described in this document are applicable for the major configurations P40C008, P40C012, P40C024, P40C040, and P40C072, in the VE edition, as well as for all minor configurations described in the *[ST]*.

Note that although AES is present and available for the TOE user in case the minor configuration option for AES is set, AES is out of scope of this evaluation, and no claims regarding resistance against attackers are made.

2.9 Results of the Evaluation

The evaluation lab documented their evaluation results in the *[ETR]*, which references an 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 NXP Secure Smart Card Controller 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 requirements specified in Security Target *[ST]*.

The Security Target claims ’strict’ conformance to the Protection Profile *[PP]*.

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.

Please note that although the TOE contains accelerators for AES, CRC and large number arithmetic, the functionality and security of these features has not been topic of this evaluation. Composite product developers should do their own security analysis and/or testing.

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 cryptographic algorithms and protocols was not rated in the course of this evaluation. This specifically applies to the following proprietary or non-standard algorithms, protocols and implementations: none.

Not all key sizes specified in the *[ST]* have sufficient cryptographic strength for satisfying the AVA_VAN.5 “high attack potential”. In order to be protected against attackers with a "high attack potential", appropriate cryptographic algorithms with sufficiently large cryptographic key sizes shall be used (references can be found in national and international documents and standards).

3 Security Target

The NXP Secure Smart Card Controller P40C008/012/024/040/072 VE.001 Security Target, Rev 3.1, 2020-12-14 *[ST]* is included here by reference.

Please note that for the need of publication a public version *[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
CRC	Cyclic Redundancy Check
DES	Data Encryption Standard
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
TRNG	True Random Number Generator
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 5, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.

[ETR] Evaluation Technical Report NXP Secure Smart Card Controller P40C008/012/024/040/072 VE.001 EAL5+, 21-RPT-050, v1.0, 18 January 2021.

[ETRfC] Evaluation Technical Report for Composite Evaluation NXP Secure Smart Card Controller P40C008/012/024/040/072 VE.001 EAL5+, 21-RPT-051, v1.0, 18 January 2021.

[JIL-AAPS] JIL Application of Attack Potential to Smartcards, Version 3.1, June 2020.

[JIL-AM] Attack Methods for Smartcards and Similar Devices, Version 2.4, January 2020 (sensitive with controlled distribution).

[NSCIB] Netherlands Scheme for Certification in the Area of IT Security, Version 2.5, 28 March 2019.

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

[ST] NXP Secure Smart Card Controller P40C008/012/024/040/072 VE.001 Security Target, Rev 3.1, 2020-12-14.

[ST-lite] NXP Secure Smart Card Controller P40C008/012/024/040/072 VE.001 Security Target Lite, Rev. 3.0, 2020-12-14.

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

(This is the end of this report).